NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
1	Definitions, abbreviations and acronyms	See FDE for details	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1
2	Scope of application and proportionality	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
3	Scope of application and proportionality	The provisions of this circular shall apply to all In-Scope Entities on an individual basis. Credit institutions and investment firms shall also comply with this circular on a sub-consolidated and consolidated basis, taking into account their prudential scope of consolidation. Credit institutions and investment firms that are a parent undertaking shall ensure that the internal governance arrangements, processes and mechanisms in their subsidiaries are consistent, well integrated and appropriate for the effective application of this circular at all relevant levels of supervision.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
4	Scope of application and proportionality	In-Scope Entities shall, when complying with this circular, have regard to the principle of proportionality. According to this principle, In-Scope Entities shall take implementing measures that are proportionate to their size and their internal organisation as well as to the nature, scale and complexity of their activities or services, including their risks. As such, In-Scope Entities that are large, complex or engage in risky activities or services shall adopt a more robust framework for their central administration, internal governance and risk management. By contrast, In-Scope Entities may apply a less elaborated framework where justified by their size and internal organisation as well as by the nature, scale and complexity of their activities or services, including	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
5	Scope of application and proportionality	That said, outsourcing arrangements may have an impact on the risk profile of the In-Scope Entities, notably the operational risk they may be exposed to (e.g. disruption risk). Consequently, In-Scope Entities may need to enhance their internal control framework and procedures to integrate this modified risk dimension into their entity-wide risk management framework.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
5	Scope of application and proportionality	That said, outsourcing arrangements may have an impact on the risk profile of the In-Scope Entities, notably the operational risk they may be exposed to (e.g. disruption risk). Consequently, In-Scope Entities may need to enhance their internal control framework and procedures to integrate this modified risk dimension into their entity-wide risk management framework.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
6	Scope of application and proportionality	To support the appropriate implementation of this circular, In-Scope Entities shall document their proportionality analysis in writing and have their conclusions approved by the management body.	Functional	Subset Of	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10		CPL-01.3
6	Scope of application and proportionality	To support the appropriate implementation of this circular, In-Scope Entities shall document their proportionality analysis in writing and have their conclusions approved by the management body.	Functional	Intersects With	Work Products	CPL-26	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5		CPL-13
7	General principles governing outsourcing arrangements	Outsourcing is a means for In-Scope Entities to get relatively easy access to expertise including in the space of new technologies and to achieve economies of scale and therefore improve cost efficiency. However, the implementation of outsourcing arrangements by In-Scope Entities creates specific risks and shall be subject to specific requirements in accordance with Articles 36-2 LFS, 37-1(5) LFS, 11(4) LPS and 24-7(4) LPS, where applicable. Outsourcing arrangements shall be subject to the following principles: - Outsourcing arrangements shall be subject to appropriate oversight and may, in no circumstances, lead to the circumvention of the spirit and letter of regulatory requirements or prudential measures. - When outsourcing operational tasks to a service provider, the In-Scope Entity shall ensure that those operational tasks are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports in line with section 4.3.3 and with section 4.2.6 and sub-section 4.3.2.3, respectively. - The responsibility of the management body for the In-Scope Entity and all its activities can never be outsourced: • Any outsourcing that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the In-Scope Entities towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the In-scope Entity's authorisation was granted, shall not be permitted. • The In-Scope Entity remains fully responsible for compliance with regulatory requirements including in the case of sub-outsourcing as sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the In-Scope Entity must determine whether sub-outsourcing is authorized and adapt its internal governance and risk management framework with regard to sub-outsourcing, in	Functional	Subset Of	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	10		TPM-01
7	General principles governing outsourcing arrangements	Outsourcing is a means for In-Scope Entities to get relatively easy access to expertise including in the space of new technologies and to achieve economies of scale and therefore improve cost efficiency. However, the implementation of outsourcing arrangements by In-Scope Entities creates specific risks and shall be subject to specific requirements in accordance with Articles 36-2 LFS, 37-1(5) LFS, 11(4) LPS and 24-7(4) LPS, where applicable. Outsourcing arrangements shall be subject to the following principles: - Outsourcing arrangements shall be subject to appropriate oversight and may, in no circumstances, lead to the circumvention of the spirit and letter of regulatory requirements or prudential measures. - When outsourcing operational tasks to a service provider, the In-Scope Entity shall ensure that those operational tasks are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports in line with section 4.3.3 and with section 4.2.6 and sub-section 4.3.2.3, respectively. - The responsibility of the management body for the In-Scope Entity and all its activities can never be outsourced: • Any outsourcing that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the In-Scope Entities towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the In-scope Entity's authorisation was granted, shall not be permitted. • The In-Scope Entity remains fully responsible for compliance with regulatory requirements including in the case of sub-outsourcing as sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the In-Scope Entity must determine whether sub-outsourcing is authorized and adapt its internal governance and risk management framework with regard to sub-outsourcing, in	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
7	General principles governing outsourcing arrangements	Outsourcing is a means for In-Scope Entities to get relatively easy access to expertise including in the space of new technologies and to achieve economies of scale and therefore improve cost efficiency. However, the implementation of outsourcing arrangements by In-Scope Entities creates specific risks and shall be subject to specific requirements in accordance with Articles 36-2 LFS, 37-1(5) LFS, 11(4) LPS and 24-7(4) LPS, where applicable. Outsourcing arrangements shall be subject to the following principles: - Outsourcing arrangements shall be subject to appropriate oversight and may, in no circumstances, lead to the circumvention of the spirit and letter of regulatory requirements or prudential measures. - When outsourcing operational tasks to a service provider, the In-Scope Entity shall ensure that those operational tasks are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports in line with section 4.3.3 and with section 4.2.6 and sub-section 4.3.2.3, respectively. - The responsibility of the management body for the In-Scope Entity and all its activities can never be outsourced: • Any outsourcing that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the In-Scope Entities towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the In-scope Entity's authorisation was granted, shall not be permitted. • The In-Scope Entity remains fully responsible for compliance with regulatory requirements including in the case of sub-outsourcing as sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the In-Scope Entity must determine whether sub-outsourcing is authorized and adapt its internal governance and risk management framework with regard to sub-outsourcing, in	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8		TPM-05
7	General principles governing outsourcing arrangements	Outsourcing is a means for In-Scope Entities to get relatively easy access to expertise including in the space of new technologies and to achieve economies of scale and therefore improve cost efficiency. However, the implementation of outsourcing arrangements by In-Scope Entities creates specific risks and shall be subject to specific requirements in accordance with Articles 36-2 LFS, 37-1(5) LFS, 11(4) LPS and 24-7(4) LPS, where applicable. Outsourcing arrangements shall be subject to the following principles: - Outsourcing arrangements shall be subject to appropriate oversight and may, in no circumstances, lead to the circumvention of the spirit and letter of regulatory requirements or prudential measures. - When outsourcing operational tasks to a service provider, the In-Scope Entity shall ensure that those operational tasks are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports in line with section 4.3.3 and with section 4.2.6 and sub-section 4.3.2.3, respectively. - The responsibility of the management body for the In-Scope Entity and all its activities can never be outsourced: • Any outsourcing that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the In-Scope Entities towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the In-scope Entity's authorisation was granted, shall not be permitted. • The In-Scope Entity remains fully responsible for compliance with regulatory requirements including in the case of sub-outsourcing as sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the In-Scope Entity must determine whether sub-outsourcing is authorized and adapt its internal governance and risk management framework with regard to sub-outsourcing, in	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
7	General principles governing outsourcing arrangements	Outsourcing is a means for In-Scope Entities to get relatively easy access to expertise including in the space of new technologies and to achieve economies of scale and therefore improve cost efficiency. However, the implementation of outsourcing arrangements by In-Scope Entities creates specific risks and shall be subject to specific requirements in accordance with Articles 36-2 LFS, 37-1(5) LFS, 11(4) LPS and 24-7(4) LPS, where applicable. Outsourcing arrangements shall be subject to the following principles: - Outsourcing arrangements shall be subject to appropriate oversight and may, in no circumstances, lead to the circumvention of the spirit and letter of regulatory requirements or prudential measures. - When outsourcing operational tasks to a service provider, the In-Scope Entity shall ensure that those operational tasks are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports in line with section 4.3.3 and with section 4.2.6 and sub-section 4.3.2.3, respectively. - The responsibility of the management body for the In-Scope Entity and all its activities can never be outsourced: • Any outsourcing that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the In-Scope Entities towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the In-scope Entity's authorisation was granted, shall not be permitted. • The In-Scope Entity remains fully responsible for compliance with regulatory requirements including in the case of sub-outsourcing as sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the In-Scope Entity must determine whether sub-outsourcing is authorized and adapt its internal governance and risk management framework with regard to sub-outsourcing, in	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
8	General principles governing outsourcing arrangements	When performing outsourcing arrangements that involve information subject to confidentiality requirements, In-Scope Entities shall put in place appropriate confidentiality arrangements and ensure compliance with Article 41(2a) LFS or Article 30(2a) LPS, where applicable.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	3		HRS-06.1
8	General principles governing outsourcing arrangements	When performing outsourcing arrangements that involve information subject to confidentiality requirements, In-Scope Entities shall put in place appropriate confidentiality arrangements and ensure compliance with Article 41(2a) LFS or Article 30(2a) LPS, where applicable.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
9	General principles governing outsourcing arrangements	In-Scope Entities shall comply with GDPR and the requirements of the Luxembourg competent authority in this area, namely the "Commission Nationale pour la Protection des Données" (CNPD).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
9	General principles governing outsourcing arrangements	In-Scope Entities shall comply with GDPR and the requirements of the Luxembourg competent authority in this area, namely the "Commission Nationale pour la Protection des Données" (CNPD).	Functional	Intersects With	Data Privacy Program	PRI-02	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and	5		PRI-01
10	General principles governing outsourcing arrangements	Outsourcing may, in no circumstances, hamper the performance of supervisory powers by competent authorities with regard to all aspects of supervisory relevance. Outsourcing arrangements shall in particular not impact the competent authorities' ability to oversee and supervise In-Scope Entities' compliance with legal or regulatory requirements under a going concern or BRRD institutions' regulatory compliance from a resolution perspective.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
10	General principles governing outsourcing arrangements	Outsourcing may, in no circumstances, hamper the performance of supervisory powers by competent authorities with regard to all aspects of supervisory relevance. Outsourcing arrangements shall in particular not impact the competent authorities' ability to oversee and supervise In-Scope Entities' compliance with legal or regulatory requirements under a going concern or BRRD institutions' regulatory compliance from a resolution perspective.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
11	Intragroup outsourcing	Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the group. Intragroup outsourcing is therefore subject to the same regulatory framework and conditions as outsourcing to service providers outside the group. Where In-Scope Entities intend to outsource to entities within the same group, they shall also ensure that the reason for selecting a group entity is based on objective reasons. In particular, the group entity shall be suitable and the outsourcing arrangement may not expose the In-Scope Entities to an undue conflict of interest.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
11	Intragroup outsourcing	Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the group. Intragroup outsourcing is therefore subject to the same regulatory framework and conditions as outsourcing to service providers outside the group. Where In-Scope Entities intend to outsource to entities within the same group, they shall also ensure that the reason for selecting a group entity is based on objective reasons. In particular, the group entity shall be suitable and the outsourcing arrangement may not expose the In-Scope Entities to an undue conflict of interest.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		TPM-04.3
12	Intragroup outsourcing	When outsourcing within the same group, In-Scope Entities may have a higher level of control over and information about the outsourced function and the service provider, which they could take into account in their risk assessment. In-Scope Entities shall however not exclusively rely on their group entities for the management of the outsourcing and shall design procedures for the performance of appropriate monitoring and oversight at the level of the In-Scope Entity itself to ensure compliance with the requirements set out in this circular.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
12	Intragroup outsourcing	When outsourcing within the same group, In-Scope Entities may have a higher level of control over and information about the outsourced function and the service provider, which they could take into account in their risk assessment. In-Scope Entities shall however not exclusively rely on their group entities for the management of the outsourcing and shall design procedures for the performance of appropriate monitoring and oversight at the level of the In-Scope Entity itself to ensure compliance with the requirements set out in this circular.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
13	Intragroup outsourcing	Subject to the general principles set out in sub-chapter 3.1, In-Scope Entities that use centrally provided governance arrangements shall therefore comply with the following:	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	GOV-03	Mechanisms exist to centrally-manage security, compliance and resilience: (1) Controls; and (2) Related processes.	3		SEA-01.1
13.a	Intragroup outsourcing	where In-Scope Entities have outsourcing arrangements with service providers within the group, the management body of the In-Scope Entity retains, also for these outsourcing arrangements, full responsibility for compliance with the regulatory requirements and the effective application of this circular;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
13.b	Intragroup outsourcing	where In-Scope Entities have outsourcing arrangements with a service provider within the group, the In-Scope Entity shall ensure that those outsourcing arrangements, including operational tasks that are outsourced, are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports, in line with section 4.3.3. and with section 4.2.6 and sub-section 4.3.2.3, respectively.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	3		CPL-02.2
13.b	Intragroup outsourcing	where In-Scope Entities have outsourcing arrangements with a service provider within the group, the In-Scope Entity shall ensure that those outsourcing arrangements, including operational tasks that are outsourced, are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports, in line with section 4.3.3. and with section 4.2.6 and sub-section 4.3.2.3, respectively.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
14	Intragroup outsourcing	In addition to point 13 above, In-Scope Entities within a group shall take into account the following:	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
14.a	Intragroup outsourcing	where the operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), In-Scope Entities shall ensure that both the independent monitoring of the service provider and its appropriate oversight by each In-Scope Entity is possible, including by receiving, at least annually and upon request, from the centralised monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring and by challenging those reports. In addition, In-Scope Entities shall receive from the centralised monitoring function a summary of the relevant outsourcing audit reports and, upon request, the full audit report. The management body of In-Scope Entities shall determine whether the extent and the contents of these reports are consistent and appropriate and shall take action if these reports do not enable it to comply with the requirements on internal governance and on risk management as laid down in other	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	3		CPL-02.2
14.a	Intragroup outsourcing	where the operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), In-Scope Entities shall ensure that both the independent monitoring of the service provider and its appropriate oversight by each In-Scope Entity is possible, including by receiving, at least annually and upon request, from the centralised monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring and by challenging those reports. In addition, In-Scope Entities shall receive from the centralised monitoring function a summary of the relevant outsourcing audit reports and, upon request, the full audit report. The management body of In-Scope Entities shall determine whether the extent and the contents of these reports are consistent and appropriate and shall take action if these reports do not enable it to comply with the requirements on internal governance and on risk management as laid down in other	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
14.a	Intragroup outsourcing	where the operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), In-Scope Entities shall ensure that both the independent monitoring of the service provider and its appropriate oversight by each In-Scope Entity is possible, including by receiving, at least annually and upon request, from the centralised monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring and by challenging those reports. In addition, In-Scope Entities shall receive from the centralised monitoring function a summary of the relevant outsourcing audit reports and, upon request, the full audit report. The management body of In-Scope Entities shall determine whether the extent and the contents of these reports are consistent and appropriate and shall take action if these reports do not enable it to comply with the requirements on internal governance and on risk management as laid down in other	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
14.b	Intragroup outsourcing	In-Scope Entities shall ensure that their management body shall be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, comprising legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes and accept them or take action as appropriate;	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
14.b	Intragroup outsourcing	In-Scope Entities shall ensure that their management body shall be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, comprising legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes and accept them or take action as appropriate;	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	8		TPM-10
14.c	Intragroup outsourcing	where In-Scope Entities within the group rely on a central pre-outsourcing assessment of outsourcing arrangements, each In-Scope Entity shall receive a summary of the assessment and ensure that it takes into consideration its specific structure and risks within the decision-making process and accept it or take action as appropriate;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8		TPM-04.1
14.d	Intragroup outsourcing	for In-Scope Entities within a group, the register as referred to in section 4.2.7 may be kept centrally. Where the register of all existing outsourcing arrangements, is established and maintained centrally within a group, the competent authorities and all In-Scope Entities shall be able to obtain the individual register without undue delay. This register shall include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group. In-Scope Entities shall be satisfied that the register complies with the provisions set out in Section 4.2.7 on Documentation requirements;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
14.e	Intragroup outsourcing	in relation to their exit strategies, where In-Scope Entities rely on an exit plan for a critical or important function that has been established at group level, all In-Scope Entities shall receive a summary of the plan and be satisfied that the plan can be effectively executed in accordance with the provisions set out in Section 4.3.4 on Exit plans;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
14.e	Intragroup outsourcing	in relation to their exit strategies, where In-Scope Entities rely on an exit plan for a critical or important function that has been established at group level, all In-Scope Entities shall receive a summary of the plan and be satisfied that the plan can be effectively executed in accordance with the provisions set out in Section 4.3.4 on Exit plans;	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7
14.e	Intragroup outsourcing	in relation to their exit strategies, where In-Scope Entities rely on an exit plan for a critical or important function that has been established at group level, all In-Scope Entities shall receive a summary of the plan and be satisfied that the plan can be effectively executed in accordance with the provisions set out in Section 4.3.4 on Exit plans;	Functional	Subset Of	Terminating Third-Party Relationships	TPM-24	Mechanisms exist to establish, maintain and execute a documented exit strategy for applicable third-party relationships prior to the cessation of third-party services to support an orderly, secure, compliant and resilient transition to another third-party or to internally-managed services.	10		
14.f	Intragroup outsourcing	In-Scope Entities within a group may rely on centrally established business continuity plans regarding their outsourced functions. In-Scope Entities shall receive a summary of the plan and be satisfied that the plan complies with the provisions of Section 4.2.5 on Business continuity plans.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
14.f	Intragroup outsourcing	In-Scope Entities within a group may rely on centrally established business continuity plans regarding their outsourced functions. In-Scope Entities shall receive a summary of the plan and be satisfied that the plan complies with the provisions of Section 4.2.5 on Business continuity plans.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
15	Outsourcing	In-Scope Entities shall establish whether an arrangement with a third party falls under the definition of outsourcing. Within this assessment, consideration shall be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by In-Scope Entities, even if the In-Scope Entity has not performed this function in the past itself.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
16	Outsourcing	Where an arrangement with a service provider covers multiple functions, In-Scope Entities shall consider all aspects of the arrangement within their assessment, e.g. if the service provided includes the provision of data storage hardware and the backup of data, both aspects shall be considered together.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
17	Outsourcing	As a general principle, In-Scope Entities shall not consider the following as outsourcing:	Functional	No Relationship	N/A	N/A	N/A	0		
17.a	Outsourcing	a function that is legally required to be performed by a service provider, e.g. statutory audit;	Functional	No Relationship	N/A	N/A	N/A	0		
17.b	Outsourcing	market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);	Functional	No Relationship	N/A	N/A	N/A	0		
17.c	Outsourcing	global network infrastructures (e.g. Visa, MasterCard);	Functional	No Relationship	N/A	N/A	N/A	0		
17.d	Outsourcing	clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;	Functional	No Relationship	N/A	N/A	N/A	0		
17.e	Outsourcing	global financial messaging infrastructures that are subject to oversight by relevant authorities;	Functional	No Relationship	N/A	N/A	N/A	0		
17.f	Outsourcing	correspondent banking services; and	Functional	No Relationship	N/A	N/A	N/A	0		
17.g	Outsourcing	the acquisition of services that would otherwise not be undertaken by the In-Scope Entity (e.g. advice from an architect, legal advice and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the In-Scope Entity's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line).	Functional	No Relationship	N/A	N/A	N/A	0		
18	Critical or important functions	In-Scope Entities shall always consider a function as critical or important in the following situations:	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
18.a	Critical or important functions	where a defect or failure in its performance would materially impair:	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
18.a.i	Critical or important functions	their continuing compliance with the conditions of their authorisation and/or their other legal and regulatory obligations;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
18.a.ii	Critical or important functions	their financial performance; or	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
18.a.iii	Critical or important functions	the soundness or continuity of their services and activities;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
18.b	Critical or important functions	when operational tasks of internal control functions or operational tasks of the financial and accounting function as referred in points 21 to 29 are outsourced;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
18.c	Critical or important functions	when credit institutions and payment institutions intend to outsource functions of banking activities or payment services to an extent that would require authorisation by the relevant competent authority as referred to in points 61 to 63.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
19	Critical or important functions	In the case of BRRD institutions, particular attention shall be given to the assessment of the criticality or importance of functions if the outsourcing concerns functions related to core business lines and critical functions according to the BRRD Law and identified by these institutions using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778. Functions that are necessary to perform activities of core business lines or critical functions shall be considered as critical or important functions for the purpose of this circular, unless the BRRD institution's assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the operational continuity of the core business line or critical	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20	Critical or important functions	When assessing whether an outsourcing arrangement relates to a function that is critical or important, In-Scope Entities shall take into account, together with the outcome of the risk assessment outlined in points 66 to 70 at least the following factors:	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.a	Critical or important functions	whether the outsourcing arrangement is directly connected to core business activities;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.b	Critical or important functions	the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
20.b	Critical or important functions	the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.b.i	Critical or important functions	short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.b.ii	Critical or important functions	business continuity and operational resilience;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5		RSK-08
20.b.ii	Critical or important functions	business continuity and operational resilience;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply	5		TPM-02
20.b.iii	Critical or important functions	operational risk, including conduct, ICT and legal risks;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.b.iv	Critical or important functions	reputational risks;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.b.v	Critical or important functions	where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
20.c	Critical or important functions	the potential impact of the outsourcing arrangement on their ability to:	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.c.i	Critical or important functions	identify, monitor and manage all risks;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.c.ii	Critical or important functions	comply with legal and regulatory requirements;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.c.iii	Critical or important functions	conduct appropriate audits regarding the outsourced function;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.d	Critical or important functions	the potential impact on the services provided to its clients;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.e	Critical or important functions	all outsourcing arrangements, the In-Scope Entity's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
20.f	Critical or important functions	the size and complexity of any business area affected;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.g	Critical or important functions	the possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.h	Critical or important functions	the ability to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability');	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.i	Critical or important functions	the ability to reintegrate the outsourced function into the In-Scope Entity, if necessary or desirable;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
20.j	Critical or important functions	the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the In-Scope Entity and its clients, including but not limited to compliance with GDPR.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
21	Outsourcing arrangements relating to internal control functions	Outsourcing arrangements of internal control functions shall not effectively result in the transfer of these functions as a whole to the service provider(s). Therefore, outsourcing arrangements shall be limited, in principle, to operational tasks of these functions.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5		GOV-19.3
22	Outsourcing arrangements relating to internal control functions	Outsourcing arrangements of operational tasks of the internal control functions shall not undermine the permanence of the internal control arrangements and functions of the In-Scope Entity or their continued effectiveness. In practice this means that outsourcing arrangements shall be proportionate and shall not result in the effective carving out of the substance of the In-Scope Entities' internal control functions.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5		GOV-19.3
23	Outsourcing arrangements relating to internal control functions	In accordance with the requirements of section 4.3.1.2, In-Scope Entities shall ascertain that the service provider complies with applicable suitability requirements and has appropriate and sufficient technical knowledge and experience. In particular, the service provider shall demonstrate an appropriate and up-to-date knowledge of the regulatory framework that applies to the In-Scope Entity.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
24	Outsourcing arrangements relating to internal control functions	When outsourcing operational tasks of the internal control functions, the service provider shall be placed under the oversight of and report to the person in charge of the relevant internal control function of the In-scope Entity (e.g. the Chief Compliance Officer, the Chief Risk Officer or the Chief Internal Auditor). Where In-scope Entities outsource the full range of operational tasks of their internal control function, the service provider shall report to the member of the management body in charge of the internal control function.	Functional	Intersects With	Authoritative Chain of Command	GOV-05.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity for individuals and teams managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.2
24	Outsourcing arrangements relating to internal control functions	When outsourcing operational tasks of the internal control functions, the service provider shall be placed under the oversight of and report to the person in charge of the relevant internal control function of the In-scope Entity (e.g. the Chief Compliance Officer, the Chief Risk Officer or the Chief Internal Auditor). Where In-scope Entities outsource the full range of operational tasks of their internal control function, the service provider shall report to the member of the management body in charge of the internal control function.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	3		TPM-05.4
24	Outsourcing arrangements relating to internal control functions	When outsourcing operational tasks of the internal control functions, the service provider shall be placed under the oversight of and report to the person in charge of the relevant internal control function of the In-scope Entity (e.g. the Chief Compliance Officer, the Chief Risk Officer or the Chief Internal Auditor). Where In-scope Entities outsource the full range of operational tasks of their internal control function, the service provider shall report to the member of the management body in charge of the internal control function.	Functional	Intersects With	Third-Party Personnel Security	TPM-13	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	3		TPM-06
25	Outsourcing arrangements relating to internal control functions	In the context of the internal audit function, the service provider shall also have a direct access to the management body in its supervisory functions or, where appropriate, to the chairperson of the audit committee. In addition, the service provider shall carry out the internal audit operational tasks in accordance with the In-Scope Entity's internal audit plan and work programme, document the work and the findings of each mission in sufficient detail and issue a dedicated report on each mission. All documents shall be drafted in French, German or English and delivered to the person in charge of the internal audit function, to the management body and, where applicable, to the	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
26	Outsourcing arrangements relating to the financial and accounting function	Outsourcing arrangements of the financial and accounting function shall not effectively result in the transfer of this function as a whole to the service provider(s). Therefore, outsourcing arrangements shall be limited, in principle, to operational tasks of this function. Outsourcing arrangements of operational tasks of the financial and accounting functions shall not undermine the permanence of the central administration of the In-Scope Entity.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
27	Outsourcing arrangements relating to the financial and accounting function	When outsourcing operational tasks of the accounting function, In-Scope Entities shall have, at the closing of each day, unconditional and unrestricted access to the balance of all accounts and of all accounting movements of the day in order to provide the competent authority or any other body, as required by applicable laws and regulations, with this information.	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-22	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	3		DCH-13

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
28	Outsourcing arrangements relating to the financial and accounting function	When using an accounting system that is located outside of Luxembourg (accounting system hosting outsourcing) independently or in connection with the outsourcing of operational tasks of the accounting function, the In-Scope Entity shall have, at the end of each day, a secure backup of all end of day accounting positions, including client positions, in a readable format, to guarantee an autonomous preparation of a balance sheet, a profit and loss statement and client positions. This backup shall be stored at the premises of the In-Scope Entity in the EEA, of a group entity located in the EEA, or of another service provider (i.e. a service provider different from the one to whom the accounting system is outsourced) located in the EEA. The accounting system shall allow keeping regular accounts in accordance with the applicable accounting framework in Luxembourg, the preparation of statutory accounts and the preparation of the prudential	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
28	Outsourcing arrangements relating to the financial and accounting function	When using an accounting system that is located outside of Luxembourg (accounting system hosting outsourcing) independently or in connection with the outsourcing of operational tasks of the accounting function, the In-Scope Entity shall have, at the end of each day, a secure backup of all end of day accounting positions, including client positions, in a readable format, to guarantee an autonomous preparation of a balance sheet, a profit and loss statement and client positions. This backup shall be stored at the premises of the In-Scope Entity in the EEA, of a group entity located in the EEA, or of another service provider (i.e. a service provider different from the one to whom the accounting system is outsourced) located in the EEA. The accounting system shall allow keeping regular accounts in accordance with the applicable accounting framework in Luxembourg, the preparation of statutory accounts and the preparation of the prudential	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
29	Outsourcing arrangements relating to the financial and accounting function	In case of outsourcing of the production of prudential reports, the person in charge of the financial and accounting function in the In-Scope Entity shall ensure that these reports represent faithfully the In-Scope Entity's prudential situation and are prepared in accordance with the applicable instructions. In addition, this person shall be able to ensure that the In-Scope Entity's annual accounts are prepared in accordance with the applicable accounting laws and regulations.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
30	Sound governance arrangements and third-party risk	As part of the overall internal control framework, including internal control mechanisms, In-Scope Entities shall have a holistic entity-wide risk management framework extending across all business lines and internal units. Under that framework, In-Scope Entities shall identify and manage all their risks, including risks caused by arrangements with third parties. The risk management framework shall also enable In-Scope Entities to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented, including with regard to cyber risks.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	8		RSK-01
30	Sound governance arrangements and third-party risk	As part of the overall internal control framework, including internal control mechanisms, In-Scope Entities shall have a holistic entity-wide risk management framework extending across all business lines and internal units. Under that framework, In-Scope Entities shall identify and manage all their risks, including risks caused by arrangements with third parties. The risk management framework shall also enable In-Scope Entities to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented, including with regard to cyber risks.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
31	Sound governance arrangements and third-party risk	In-Scope Entities, taking into account the principle of proportionality, shall identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed, regardless of whether or not those arrangements are outsourcing arrangements. The risks, in particular the operational risks, of all arrangements with third parties, shall be assessed in line with points 66 to 70.	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
31	Sound governance arrangements and third-party risk	In-Scope Entities, taking into account the principle of proportionality, shall identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed, regardless of whether or not those arrangements are outsourcing arrangements. The risks, in particular the operational risks, of all arrangements with third parties, shall be assessed in line with points 66 to 70.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03
32	Sound governance arrangements and third-party risk	In-Scope Entities shall ensure that they comply with all requirements under GDPR, including for their third-party and outsourcing arrangements.	Functional	Intersects With	Data Privacy Program	PRI-02	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and	5		PRI-01
32	Sound governance arrangements and third-party risk	In-Scope Entities shall ensure that they comply with all requirements under GDPR, including for their third-party and outsourcing arrangements.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5		PRI-07.1
33	Sound governance arrangements for outsourcing	The outsourcing of functions shall not result in the delegation of the management body's responsibilities. The management body remains fully responsible and accountable for complying with all of their regulatory obligations or their responsibilities to their customers, including the ability to oversee the outsourcing of critical or important functions.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
34	Sound governance arrangements for outsourcing	The management body is at all times fully responsible and accountable for at least:	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
34.a	Sound governance arrangements for outsourcing	ensuring that the In-Scope Entity meets on an ongoing basis the conditions with which it must comply to remain authorised, including any conditions imposed by the competent authority;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
34.b	Sound governance arrangements for outsourcing	the internal organisation of the In-Scope Entity;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.1
34.c	Sound governance arrangements for outsourcing	the identification, assessment and management of conflicts of interest;	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	3		TPM-04.3
34.d	Sound governance arrangements for outsourcing	the setting of the In-Scope Entity's strategies and policies (e.g. the business model, the risk appetite, the risk management framework);	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
34.d	Sound governance arrangements for outsourcing	the setting of the In-Scope Entity's strategies and policies (e.g. the business model, the risk appetite, the risk management framework);	Functional	Intersects With	Risk Appetite	RSK-05.3	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	3		RSK-01.5
34.e	Sound governance arrangements for outsourcing	overseeing the day-to-day management of the In-Scope Entity, including the management of all risks associated with outsourcing; and	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.1
34.e	Sound governance arrangements for outsourcing	overseeing the day-to-day management of the In-Scope Entity, including the management of all risks associated with outsourcing; and	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
34.f	Sound governance arrangements for outsourcing	the oversight role of the management body in its supervisory function, including overseeing and monitoring management decision-making.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.1
35	Sound governance arrangements for outsourcing	Outsourcing shall not lower the suitability requirements applied to the In-Scope Entity's management body and key function holders. In-Scope Entities shall have adequate competence, sufficient and appropriately skilled resources to ensure an appropriate management and oversight of outsourcing arrangements.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
35	Sound governance arrangements for outsourcing	Outsourcing shall not lower the suitability requirements applied to the In-Scope Entity's management body and key function holders. In-Scope Entities shall have adequate competence, sufficient and appropriately skilled resources to ensure an appropriate management and oversight of outsourcing arrangements.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
36	Sound governance arrangements for outsourcing	In-Scope Entities shall:	Functional	No Relationship	N/A	N/A	N/A	0		
36.a	Sound governance arrangements for outsourcing	clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
36.a	Sound governance arrangements for outsourcing	clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
36.b	Sound governance arrangements for outsourcing	allocate sufficient skilled resources to ensure compliance with the legal and regulatory requirements, including this circular and the documentation and monitoring all outsourcing arrangements;	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5		PRM-03
36.c	Sound governance arrangements for outsourcing	for each outsourced activity, designate from among its employees a person who will be in charge of managing the outsourcing relationship(s) and managing access to confidential data; and	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
36.c	Sound governance arrangements for outsourcing	for each outsourced activity, designate from among its employees a person who will be in charge of managing the outsourcing relationship(s) and managing access to confidential data; and	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
36.d	Sound governance arrangements for outsourcing	establish an outsourcing function or designate a sufficiently senior staff member who is directly accountable to the management body (e.g. a key function holder of a control function) and responsible for managing and overseeing the risks of outsourcing arrangements as part of the In-Scope Entity's internal control framework and overseeing the documentation of outsourcing arrangements. Small entities shall at least ensure a clear and sound division of tasks and responsibilities for the management and control of outsourcing arrangements and may assign the outsourcing function to a member of the In-Scope Entity's management body.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
36.d	Sound governance arrangements for outsourcing	establish an outsourcing function or designate a sufficiently senior staff member who is directly accountable to the management body (e.g. a key function holder of a control function) and responsible for managing and overseeing the risks of outsourcing arrangements as part of the In-Scope Entity's internal control framework and overseeing the documentation of outsourcing arrangements. Small entities shall at least ensure a clear and sound division of tasks and responsibilities for the management and control of outsourcing arrangements and may assign the outsourcing function to a member of the In-Scope Entity's management body.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
37	Sound governance arrangements for outsourcing	In-Scope Entities shall maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities'. To this end, they shall:	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
37.a	Sound governance arrangements for outsourcing	meet all the conditions of their authorisation at all times, including the management body effectively carrying out its responsibilities as set out in point 34;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
37.b	Sound governance arrangements for outsourcing	retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements;	Functional	Intersects With	Authoritative Chain of Command	GOV-05.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity for individuals and teams managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.2
37.c	Sound governance arrangements for outsourcing	exercise appropriate oversight and be able to manage the risks that are generated by the outsourcing of critical or important functions, in particular where operational tasks of internal control functions, of the financial and accounting function or of core business activities are outsourced; and	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
37.c	Sound governance arrangements for outsourcing	exercise appropriate oversight and be able to manage the risks that are generated by the outsourcing of critical or important functions, in particular where operational tasks of internal control functions, of the financial and accounting function or of core business activities are outsourced; and	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
37.d	Sound governance arrangements for outsourcing	have sufficient skilled resources and capacities to ensure compliance with points a. to c. above.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
37.d	Sound governance arrangements for outsourcing	have sufficient skilled resources and capacities to ensure compliance with points a. to c. above.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
38	Sound governance arrangements for outsourcing	When setting up an outsourcing arrangement, In-Scope Entities shall at least ensure that:	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
38.a	Sound governance arrangements for outsourcing	they can take and implement decisions related to their business activities and critical or important functions, including with regard to those that have been outsourced;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
38.b	Sound governance arrangements for outsourcing	they maintain the orderliness of the conduct of their business and, for credit institutions and payment institutions, the banking and payment services they provide;	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
38.c	Sound governance arrangements for outsourcing	the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech);	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
38.c	Sound governance arrangements for outsourcing	the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech);	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03
38.d	Sound governance arrangements for outsourcing	appropriate confidentiality arrangements are in place regarding data and other information;	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	5		HRS-06.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
38.e	Sound governance arrangements for outsourcing	an appropriate flow of relevant information with service providers is maintained;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
38.f	Sound governance arrangements for outsourcing	with regard to the outsourcing of critical or important functions, they are able to undertake at least one of the following actions, within an appropriate time frame:	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
38.f.i	Sound governance arrangements for outsourcing	transfer the function to alternative service providers;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
38.f.ii	Sound governance arrangements for outsourcing	reintegrate the function; or	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	3		BCD-02.2
38.f.iii	Sound governance arrangements for outsourcing	discontinue the business activities that are depending on the function.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
38.g	Sound governance arrangements for outsourcing	where personal data are processed by service providers located in the EEA and/or third countries, appropriate measures are implemented and data are processed in accordance with GDPR;	Functional	Intersects With	External Transfer of Sensitive / Regulated Data	DCH-32	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data: (1) Cross-border; and/or (2) Interorganizational.	5		DCH-25
38.g	Sound governance arrangements for outsourcing	where personal data are processed by service providers located in the EEA and/or third countries, appropriate measures are implemented and data are processed in accordance with GDPR;	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5		PRI-07.1
38.h	Sound governance arrangements for outsourcing	appropriate confidentiality arrangements are in place and ensure compliance with Article 41(2a) LFS or Article 30(2a) LPS, where applicable.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	5		HRS-06.1
39	Outsourcing policy	The management body of an In-Scope Entity that has outsourcing arrangements in place or plans on entering into such arrangements shall approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. For credit institutions and investment firms, the outsourcing policy shall, in particular, take into account the requirements pertaining to "New Product Approval Process".	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
39	Outsourcing policy	The management body of an In-Scope Entity that has outsourcing arrangements in place or plans on entering into such arrangements shall approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. For credit institutions and investment firms, the outsourcing policy shall, in particular, take into account the requirements pertaining to "New Product Approval Process".	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	3		GOV-03
39	Outsourcing policy	The management body of an In-Scope Entity that has outsourcing arrangements in place or plans on entering into such arrangements shall approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. For credit institutions and investment firms, the outsourcing policy shall, in particular, take into account the requirements pertaining to "New Product Approval Process".	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
40	Outsourcing policy	The policy shall include the main phases of the life cycle of outsourcing arrangements and define the principles, responsibilities and processes in relation to outsourcing. In particular, the policy shall cover at least:	Functional	Intersects With	Third-Party Management Policy	TPM-01	Mechanisms exist to establish a formal, documented third-party management policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	5		
40.a	Outsourcing policy	the responsibilities of the management body in line with points 33 and 34, including its involvement, as appropriate, in the decision-making on outsourcing of critical or important functions;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.1
40.a	Outsourcing policy	the responsibilities of the management body in line with points 33 and 34, including its involvement, as appropriate, in the decision-making on outsourcing of critical or important functions;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
40.b	Outsourcing policy	the involvement of business lines, internal control functions and other individuals in respect of outsourcing arrangements;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
40.c	Outsourcing policy	the planning of outsourcing arrangements, including:	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
40.c.i	Outsourcing policy	the definition of business requirements regarding outsourcing arrangements;	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	3		TPM-03.1
40.c.ii	Outsourcing policy	the criteria, including those referred to in points 18 to 20, and processes for identifying critical or important functions;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
40.c.iii	Outsourcing policy	risk identification, assessment and management in accordance with points 66 to 70;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
40.c.iv	Outsourcing policy	due diligence checks on prospective service providers, including the measures required under points 71 to 75;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
40.c.v	Outsourcing policy	procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with points 43 to 46;	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		TPM-04.3
40.c.vi	Outsourcing policy	business continuity planning in accordance with points 47 to 50;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
40.c.vii	Outsourcing policy	the approval process of new outsourcing arrangements. This process must consider the additional time requirement due to the prior notification to the competent authority in accordance with points 59 and 60;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
40.d	Outsourcing policy	the implementation, monitoring and management of outsourcing arrangements, including:	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
40.d.i	Outsourcing policy	the ongoing assessment of the service provider's performance in line with points 104 to 110;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
40.d.ii	Outsourcing policy	the procedures for being notified and responding to changes to an outsourcing arrangement or service provider (e.g. to its financial position, organisational or ownership structures, sub-outsourcing);	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5		TPM-10
40.d.iii	Outsourcing policy	the independent review and audit of compliance with legal and regulatory requirements and policies;	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
40.d.iv	Outsourcing policy	the renewal processes;	Functional	Intersects With	Third-Party Scope Review	TPM-16	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices; (3) Applicable stakeholders; and (4) Deployed Technology Assets, Applications and/or	3		TPM-05.5
40.e	Outsourcing policy	the documentation and record-keeping, taking into account the requirements set out in points 53 to 58;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
40.f	Outsourcing policy	the exit strategies and termination processes, including a requirement for a documented exit plan for each critical or important function to be outsourced where such an exit is considered possible, taking into account possible service interruptions or the unexpected termination of an outsourcing agreement, in line with points 111 to 113.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
40.f	Outsourcing policy	the exit strategies and termination processes, including a requirement for a documented exit plan for each critical or important function to be outsourced where such an exit is considered possible, taking into account possible service interruptions or the unexpected termination of an outsourcing agreement, in line with points 111 to 113.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7
41	Outsourcing policy	The outsourcing policy shall differentiate between the following:	Functional	Intersects With	Third-Party Management Policy	TPM-01	Mechanisms exist to establish a formal, documented third-party management policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	3		
41.a	Outsourcing policy	outsourcing of critical or important functions and other outsourcing arrangements;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
41.a	Outsourcing policy	outsourcing of critical or important functions and other outsourcing arrangements;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
41.b	Outsourcing policy	outsourcing to service providers that are authorised by a relevant competent authority in a Member State or in a third country and those that are not;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
41.c	Outsourcing policy	intragroup outsourcing arrangements and outsourcing to entities outside the group; and	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
41.d	Outsourcing policy	outsourcing to service providers located within a Member State and third countries.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
41.d	Outsourcing policy	outsourcing to service providers located within a Member State and third countries.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
42	Outsourcing policy	In-Scope Entities shall ensure that the outsourcing policy covers the identification of the following potential effects of critical or important outsourcing arrangements and that these are taken into account in the decision-making process:	Functional	Intersects With	Third-Party Management Policy	TPM-01	Mechanisms exist to establish a formal, documented third-party management policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	3		
42.a	Outsourcing policy	the In-Scope Entity's risk profile;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
42.b	Outsourcing policy	the ability to oversee the service provider and to manage the risks;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
42.c	Outsourcing policy	the business continuity measures; and	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
42.d	Outsourcing policy	the performance of their business activities.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
43	Conflicts of interests	In-Scope Entities shall identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		TPM-04.3
44	Conflicts of interests	Where outsourcing creates material conflicts of interest, including between entities within the same group, In-Scope Entities need to take appropriate measures to manage those conflicts of interest.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		TPM-04.3
45	Conflicts of interests	When functions are provided by a service provider that is part of a group or that is owned by the In-Scope Entity or its group, the conditions, including financial conditions, for the outsourced service shall be set at arm's length. However, within the pricing of services synergies resulting from providing the same or similar services to several In-Scope Entities within a group may be factored in, as long as the service provider remains viable on a stand-alone basis; within a group this shall be irrespective of the failure of any other group entity.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	3		TPM-04.3
46	Conflicts of interests	The In-Scope Entity shall, in particular, ensure that the service provider is independent from the statutory auditor (réviseur d'entreprises agréé or cabinet de révision agréé) in charge of the statutory audit of the In-Scope Entity and from the group to which the statutory auditor belongs.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	3		TPM-04.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
47	Business continuity plans	Special attention shall be paid to the continuity aspects and the revocable nature of an outsourcing arrangement. The In-Scope Entity shall be able to continue its critical functions in case of exceptional events or crisis.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
48	Business continuity plans	In-Scope Entities shall have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
48	Business continuity plans	In-Scope Entities shall have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
49	Business continuity plans	Business continuity plans shall take into account the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. Such plans shall also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risks in the service provider's jurisdiction.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
49	Business continuity plans	Business continuity plans shall take into account the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. Such plans shall also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risks in the service provider's jurisdiction.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
50	Business continuity plans	Where the outsourcing arrangement comprises ICT systems and data of In-Scope Entities, the measures for redundancy and backup of these systems and data shall either be specified in the outsourcing agreement with the service provider or configured by the In-Scope Entities, in line with the business continuity plan of the In-Scope Entities.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
50	Business continuity plans	Where the outsourcing arrangement comprises ICT systems and data of In-Scope Entities, the measures for redundancy and backup of these systems and data shall either be specified in the outsourcing agreement with the service provider or configured by the In-Scope Entities, in line with the business continuity plan of the In-Scope	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
51	Internal audit function	The internal audit function's activities shall cover, following a risk-based approach, the review of outsourced activities. The audit plan and programme shall include, in particular, the outsourcing arrangements of critical or important functions.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52	Internal audit function	With regard to the outsourcing process, the internal audit function shall at least ascertain:	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52.a	Internal audit function	that the In-Scope Entity's framework for outsourcing, including the outsourcing policy, is effectively implemented and is in line with the applicable laws and regulations, the risk strategy and the decisions of the management body;	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52.a	Internal audit function	that the In-Scope Entity's framework for outsourcing, including the outsourcing policy, is effectively implemented and is in line with the applicable laws and regulations, the risk strategy and the decisions of the management body;	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	3		CPL-02.2
52.b	Internal audit function	the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52.b	Internal audit function	the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
52.c	Internal audit function	the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the In-Scope Entity's risk strategy;	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52.c	Internal audit function	the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the In-Scope Entity's risk strategy;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
52.d	Internal audit function	the appropriate involvement of governance bodies; and	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52.d	Internal audit function	the appropriate involvement of governance bodies; and	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.1
52.e	Internal audit function	the appropriate monitoring and management of outsourcing arrangements.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
52.e	Internal audit function	the appropriate monitoring and management of outsourcing arrangements.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
53	Documentation requirements	In-Scope Entities shall maintain an updated register of information on all outsourcing arrangements at individual level and, as applicable, at sub-consolidated and consolidated levels, as set out in point 3, and shall appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. In-Scope Entities shall maintain the documentation of ended outsourcing arrangements within the register and the supporting documentation for an appropriate period in accordance with Luxembourg law.	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-18
53	Documentation requirements	In-Scope Entities shall maintain an updated register of information on all outsourcing arrangements at individual level and, as applicable, at sub-consolidated and consolidated levels, as set out in point 3, and shall appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. In-Scope Entities shall maintain the documentation of ended outsourcing arrangements within the register and the supporting documentation for an appropriate period in accordance with Luxembourg law.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8		TPM-01.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
54	Documentation requirements	For the purposes of prudential supervision, the register shall include at least the following information for all existing outsourcing arrangements:	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.a	Documentation requirements	a reference number for each outsourcing arrangement;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.b	Documentation requirements	the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the In-Scope Entity;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.c	Documentation requirements	a brief description of the outsourced function, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.d	Documentation requirements	a category assigned by the In-Scope Entity that reflects the nature of the function as described under point (c) (e.g. ICT, internal control functions), which shall facilitate the identification of different types of arrangements;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.e	Documentation requirements	the name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any);	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.f	Documentation requirements	the country or countries where the service is to be performed, including the location (i.e. country or region) of the data;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.f	Documentation requirements	the country or countries where the service is to be performed, including the location (i.e. country or region) of the data;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
54.g	Documentation requirements	whether or not (yes/no) the outsourced function is considered critical or important, including a brief summary of the reasons why the outsourced function is considered or not as critical or important;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.g	Documentation requirements	whether or not (yes/no) the outsourced function is considered critical or important, including a brief summary of the reasons why the outsourced function is considered or not as critical or important;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
54.h	Documentation requirements	in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
54.h	Documentation requirements	in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.i	Documentation requirements	the date of the most recent assessment of the criticality or importance of the outsourced function.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
54.i	Documentation requirements	the date of the most recent assessment of the criticality or importance of the outsourced function.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
55	Documentation requirements	For the outsourcing of critical or important functions, the register shall include the following additional information:	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.a	Documentation requirements	the In-Scope Entities and other firms within the scope of the prudential consolidation, as applicable, that make use of the outsourcing;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.b	Documentation requirements	whether or not the service provider or sub-contractor is part of the group or is owned by In-Scope Entities within the group;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.c	Documentation requirements	the date of the most recent risk assessment and a brief summary of the main results;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.c	Documentation requirements	the date of the most recent risk assessment and a brief summary of the main results;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
55.d	Documentation requirements	the individual or decision-making body (e.g. the management body) in the In-Scope Entity that approved the outsourcing arrangement;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.e	Documentation requirements	the governing law of the outsourcing agreement;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
55.f	Documentation requirements	the dates of the most recent and next scheduled audits, where applicable;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.g	Documentation requirements	where applicable, the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including the country where the sub-contractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.h	Documentation requirements	an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the In-Scope Entity or the impact of discontinuing the critical or important function;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.h	Documentation requirements	an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the In-Scope Entity or the impact of discontinuing the critical or important function;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
55.i	Documentation requirements	identification of alternative service providers in line with point (h);	Functional	Intersects With	Separation of Primary / Alternate Providers	BCD-17.2	Mechanisms exist to reduce threat susceptibility by obtaining services from alternative providers that are different from the primary service providers.	5		BCD-10.2
55.i	Documentation requirements	identification of alternative service providers in line with point (h);	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the	5		TPM-01.1
55.j	Documentation requirements	whether the outsourced critical or important function supports business operations that are time-critical;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
55.k	Documentation requirements	the estimated annual budget cost;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
55.l	Documentation requirements	the date of the prior notification to the competent authority in accordance with points 59 and 60, as applicable.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
56	Documentation requirements	In-Scope Entities shall, upon request, make available to the competent authority either the full register of all existing outsourcing arrangements or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point 54(d) (e.g. all ICT outsourcing arrangements).	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.3
56	Documentation requirements	In-Scope Entities shall, upon request, make available to the competent authority either the full register of all existing outsourcing arrangements or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point 54(d) (e.g. all ICT outsourcing arrangements).	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
57	Documentation requirements	In-Scope Entities shall appropriately document the assessments made under points 66 to 103 and the results of their ongoing monitoring (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).	Functional	Intersects With	Defensible Evidence of Due Diligence	CPL-26.1	Mechanisms exist to produce evidence of due diligence activities performed that is capable of withstanding external audit or regulatory scrutiny.	5		CPL-13.1
57	Documentation requirements	In-Scope Entities shall appropriately document the assessments made under points 66 to 103 and the results of their ongoing monitoring (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
58	Documentation requirements	In-Scope Entities shall, upon request, make available to the competent authority all information necessary to enable the competent authority to execute its effective supervision, including a copy of the outsourcing agreement.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.3
59	Supervisory conditions for outsourcing	An In-Scope Entity that intends to outsource a critical or important function shall notify in advance its plans to the competent authority using the instructions and, where available, the forms on the CSSF website. Such a notification is to be submitted at least three (3) months before the planned outsourcing comes into effect. When resorting to a Luxembourg support PFS governed by Articles 29-1 to 29-6 LFS, this notice period is reduced to one (1) month. Any planned outsourcing arrangement which has not been notified within the above notification period and/or without using the instructions and, where applicable, the forms available on the CSSF website will be considered as not notified.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
60	Supervisory conditions for outsourcing	The notification is without prejudice to the supervisory measures or the application of binding measures and/or administrative sanctions which the competent authority might take as part of its ongoing supervision, where it appears that these outsourcing projects do not comply with the applicable legal and regulatory framework. In any event, In-Scope Entities remain fully responsible to comply with all the relevant laws and regulations as regards the planned outsourcing projects.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
61	Supervisory conditions for outsourcing	Should credit institutions or payment institutions outsource functions of banking activities or payment services to a service provider located in Luxembourg or another Member State, to an extent that the performance of that function would require authorisation or registration where such activities would be carried out in Luxembourg, such an outsourcing shall take place only if one of the following conditions is met:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
61.a	Supervisory conditions for outsourcing	the service provider is authorised or registered by a relevant competent authority in that Member State to perform such banking activities or payment services; or	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
61.b	Supervisory conditions for outsourcing	the service provider is otherwise allowed to carry out those banking activities or payment services in accordance with the relevant national legal framework.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
62	Supervisory conditions for outsourcing	Should credit institutions or payment institutions outsource functions of banking activities or payment services to a service provider located in a third country, to an extent that the performance of that function would require authorisation or registration where such activities would be carried out in Luxembourg, such an outsourcing shall take place only if the following conditions are met:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
62.a	Supervisory conditions for outsourcing	the service provider is authorised or registered to provide that banking activity or payment service in the third country and is supervised by a relevant competent authority in that third country (referred to as a 'supervisory authority'); and	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
62.b	Supervisory conditions for outsourcing	there is an appropriate cooperation agreement, e.g. in the form of a memorandum of understanding or college agreement, between the competent authority and the supervisory authorities responsible for the supervision of the service provider. In-Scope Entities shall contact the CSSF in the early planning stages of their planned outsourcing arrangement to ascertain that cooperation arrangements between the CSSF and the third country supervisory authority are or can be put in place.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
63	Supervisory conditions for outsourcing	For the purposes of points 61 and 62, the outsourcing of functions of banking activities to an extent that the performance of that function would require authorisation or registration where such activities would be carried out in Luxembourg shall apply in the event where a credit institution intends to proceed to the outsourcing of a material proportion of the activity that consists in the taking of deposits and other repayable funds from the public.	Functional	No Relationship	N/A	N/A	N/A	0		
64	Supervisory conditions for outsourcing	The outsourcing to a service provider located in Luxembourg that relates to services subject to an authorisation requirement in accordance with Articles 29-1 to 29-6 LFS shall take place only if one of the following conditions is met:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
64.a	Supervisory conditions for outsourcing	the service provider is authorised by the CSSF in accordance with Articles 29-1 to 29-6 LFS to provide such services; or	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
64.b	Supervisory conditions for outsourcing	the service provider is otherwise allowed to carry out those services, i.e. it is a credit institution or it is an entity falling under the scope of Article 1-1(2)(c) LFS that is part of the group to which the In-Scope Entity belongs and which exclusively deals with group transactions.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
65	Pre-outsourcing analysis	Before entering into any outsourcing arrangement, In-Scope Entities shall:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
65.a	Pre-outsourcing analysis	assess if the outsourcing arrangement concerns a critical or important function;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
65.b	Pre-outsourcing analysis	assess if the supervisory conditions for outsourcing are met;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
65.b	Pre-outsourcing analysis	assess if the supervisory conditions for outsourcing are met;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
65.c	Pre-outsourcing analysis	identify and assess all of the relevant risks of the outsourcing arrangement;	Functional	Subset Of	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10		TPM-04.1
65.d	Pre-outsourcing analysis	undertake appropriate due diligence on the prospective service provider; and	Functional	Intersects With	Defensible Evidence of Due Diligence	CPL-26.1	Mechanisms exist to produce evidence of due diligence activities performed that is capable of withstanding external audit or regulatory scrutiny.	3		CPL-13.1
65.d	Pre-outsourcing analysis	undertake appropriate due diligence on the prospective service provider; and	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
65.e	Pre-outsourcing analysis	identify and assess conflicts of interest that the outsourcing may cause.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		TPM-04.3
66	Risk assessment of outsourcing arrangements	In-Scope Entities shall assess the potential impact of outsourcing arrangements on their operational capacity and risk, shall take into account the assessment results when deciding if the function shall be outsourced to a service provider and shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
66	Risk assessment of outsourcing arrangements	In-Scope Entities shall assess the potential impact of outsourcing arrangements on their operational capacity and risk, shall take into account the assessment results when deciding if the function shall be outsourced to a service provider and shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
67	Risk assessment of outsourcing arrangements	The assessment shall include, where appropriate, scenarios of possible risk events, including high-severity operational risk events, in particular when the outsourcing arrangement relates to a critical or important function of the In-Scope Entity. Within the scenario analysis, In-Scope Entities shall assess the potential impact of failed or inadequate services, including the risks caused by processes, systems, people or external events. In-Scope Entities shall document the analysis performed and their results and shall estimate the extent to which the outsourcing arrangement would increase or decrease their operational risk. Small entities may use qualitative risk assessment approaches, while other In-Scope Entities shall have a more sophisticated approach, including, where available, the use of internal and external loss data to inform the scenario analysis.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
67	Risk assessment of outsourcing arrangements	The assessment shall include, where appropriate, scenarios of possible risk events, including high-severity operational risk events, in particular when the outsourcing arrangement relates to a critical or important function of the In-Scope Entity. Within the scenario analysis, In-Scope Entities shall assess the potential impact of failed or inadequate services, including the risks caused by processes, systems, people or external events. In-Scope Entities shall document the analysis performed and their results and shall estimate the extent to which the outsourcing arrangement would increase or decrease their operational risk. Small entities may use qualitative risk assessment approaches, while other In-Scope Entities shall have a more sophisticated approach, including, where available, the use of internal and external loss data to inform the scenario analysis.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
68	Risk assessment of outsourcing arrangements	When carrying out the risk assessment prior to outsourcing and during ongoing monitoring of the service provider's performance, In-Scope Entities shall, at least:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
68.a	Risk assessment of outsourcing arrangements	identify and classify the relevant functions and related data and systems as regards their risk sensitivity and required security measures;	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
68.a	Risk assessment of outsourcing arrangements	identify and classify the relevant functions and related data and systems as regards their risk sensitivity and required security measures;	Functional	Intersects With	Risk-Based Security Categorization	RSK-07	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5		RSK-02
68.b	Risk assessment of outsourcing arrangements	conduct a thorough risk-based analysis of the functions and related data and systems that are being considered for outsourcing or have been outsourced in order to address the potential risks, in particular the operational risks, including legal, ICT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are or may be provided and where the data are or are likely to be stored;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8		TPM-04.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
68.c	Risk assessment of outsourcing arrangements	consider the consequences of where the service provider is located (within or outside the EEA) in accordance with points 61 to 64 and whether the service provider is supervised by a relevant competent authority;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
68.d	Risk assessment of outsourcing arrangements	consider the political stability and security situation of the jurisdictions in question, including:	Functional	Intersects With	Data Localization	DCH-31	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		DCH-26
68.d	Risk assessment of outsourcing arrangements	consider the political stability and security situation of the jurisdictions in question, including:	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
68.d.i	Risk assessment of outsourcing arrangements	the laws in force, including laws on data protection;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
68.d.ii	Risk assessment of outsourcing arrangements	the law enforcement provisions in place; and	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
68.d.iii	Risk assessment of outsourcing arrangements	the insolvency law provisions that would apply in the event of a service provider's failure and any constraints that would arise in respect of the urgent recovery of the In-Scope Entity's data in particular;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
68.e	Risk assessment of outsourcing arrangements	define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the (intended) outsourcing. In-Scope Entities shall also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture;	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01
68.e	Risk assessment of outsourcing arrangements	define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the (intended) outsourcing. In-Scope Entities shall also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
68.e	Risk assessment of outsourcing arrangements	define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the (intended) outsourcing. In-Scope Entities shall also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture;	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5		DCH-01.2
68.f	Risk assessment of outsourcing arrangements	consider whether the service provider is a subsidiary or parent undertaking of the In-Scope Entity or is included in the scope of accounting consolidation and, if so, the extent to which the In-Scope Entity controls it or has the ability to influence its actions.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
69	Risk assessment of outsourcing arrangements	Within the risk assessment, In-Scope Entities shall also take into account the expected benefits and costs of the proposed outsourcing arrangement, including weighing any risks that may be reduced or better managed against any risks that may arise as a result of the proposed outsourcing arrangement, taking into account at least:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
69.a	Risk assessment of outsourcing arrangements	concentration risks, including from:	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
69.a	Risk assessment of outsourcing arrangements	concentration risks, including from:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
69.a.i	Risk assessment of outsourcing arrangements	outsourcing to a dominant service provider that is not easily substitutable; and	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
69.a.ii	Risk assessment of outsourcing arrangements	multiple outsourcing arrangements with the same service provider or closely connected service providers;	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
69.b	Risk assessment of outsourcing arrangements	the aggregated risks resulting from outsourcing several functions across the In-Scope Entity and, in the case of groups of In-Scope Entities, the aggregated risks on a consolidated basis;	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	3		RSK-09.1
69.b	Risk assessment of outsourcing arrangements	the aggregated risks resulting from outsourcing several functions across the In-Scope Entity and, in the case of groups of In-Scope Entities, the aggregated risks on a consolidated basis;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
69.c	Risk assessment of outsourcing arrangements	in the case of significant In-Scope Entities, the step-in risk, i.e. the risk that may result from the need to provide financial support to a service provider in distress or to take over its business operations; and	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
69.d	Risk assessment of outsourcing arrangements	the measures implemented by the In-Scope Entity and by the service provider to manage and mitigate the risks.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	3		RSK-06
69.d	Risk assessment of outsourcing arrangements	the measures implemented by the In-Scope Entity and by the service provider to manage and mitigate the risks.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
70	Risk assessment of outsourcing arrangements	Where the outsourcing arrangement includes the possibility that the service provider sub-outsources critical or important functions, or material parts thereof, to other service providers, In-Scope Entities shall take into account:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
70.a	Risk assessment of outsourcing arrangements	the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
70.a	Risk assessment of outsourcing arrangements	the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
70.b	Risk assessment of outsourcing arrangements	the risk that long and complex chains of sub-outsourcing reduce their ability to oversee the outsourced critical or important function and the ability of competent authorities to effectively supervise them.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
70.b	Risk assessment of outsourcing arrangements	the risk that long and complex chains of sub-outsourcing reduce their ability to oversee the outsourced critical or important function and the ability of competent authorities to effectively supervise them.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
71	Due diligence	Before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, In-Scope Entities shall ensure in their selection and assessment process that the service provider is suitable.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
71	Due diligence	Before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, In-Scope Entities shall ensure in their selection and assessment process that the service provider is suitable.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
72	Due diligence	In-Scope Entities shall ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, ICT, financial), the organisational structure and, if applicable, the required regulatory authorisation(s) or registration(s) to perform the function in a reliable and professional manner to meet its obligations over the duration of	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
73	Due diligence	Additional factors to be considered when conducting due diligence on a potential service provider include, but are not limited to:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
73.a	Due diligence	its business model, nature, scale, complexity, financial situation, ownership and group structure;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
73.b	Due diligence	the long-term relationships with service providers that have already been assessed and perform services for the In-Scope Entity;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
73.b	Due diligence	the long-term relationships with service providers that have already been assessed and perform services for the In-Scope Entity;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
73.c	Due diligence	whether the service provider is a parent undertaking or subsidiary of the In-Scope Entity or is part of the scope of accounting consolidation of the In-Scope Entity;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
73.d	Due diligence	whether or not the service provider is supervised by relevant competent authorities.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
74	Due diligence	Where outsourcing involves the processing of personal or confidential data, In-Scope Entities shall be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.	Functional	Intersects With	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-22.2	Mechanisms exist to ensure that the requirements for the protection of sensitive and/or regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.	8		DCH-13.3
74	Due diligence	Where outsourcing involves the processing of personal or confidential data, In-Scope Entities shall be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5		PRI-07.1
75	Due diligence	In-Scope Entities shall take appropriate steps to ensure that service providers act in a manner consistent with their values and code of conduct. In particular, with regard to service providers located in third countries and, if applicable, their sub-contractors, In-Scope Entities shall be satisfied that the service provider acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.	Functional	Intersects With	Conflict of Interests	TPM-12.1	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	3		TPM-04.3
76	Contractual phase	The rights and obligations of the In-Scope Entity and the service provider shall be clearly allocated and set out in a written outsourcing agreement.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	8		TPM-05
77	Contractual phase	The outsourcing agreement shall set out:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
77.a	Contractual phase	a clear description of the outsourced function to be provided;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
77.b	Contractual phase	the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the In-Scope Entity;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.c	Contractual phase	the governing law of the agreement;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.d	Contractual phase	the parties' financial obligations;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.e	Contractual phase	whether the sub-outsourcing, in particular, of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in points 78 to 82 that the sub-outsourcing is subject to;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.e	Contractual phase	whether the sub-outsourcing, in particular, of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in points 78 to 82 that the sub-outsourcing is subject to;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
77.f	Contractual phase	the location(s) (i.e. regions or countries) where the function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the In-Scope Entity if the service provider proposes to change the location(s);	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
77.f	Contractual phase	the location(s) (i.e. regions or countries) where the function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the In-Scope Entity if the service provider proposes to change the location(s);	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.g	Contractual phase	where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in points 83 to 87;	Functional	Intersects With	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-22.2	Mechanisms exist to ensure that the requirements for the protection of sensitive and/or regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.	5		DCH-13.3
77.g	Contractual phase	where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in points 83 to 87;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
77.h	Contractual phase	the right of the In-Scope Entity to monitor the service provider's performance on an ongoing basis;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
77.h	Contractual phase	the right of the In-Scope Entity to monitor the service provider's performance on an ongoing basis;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
77.i	Contractual phase	the agreed service levels, which shall include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
77.j	Contractual phase	the reporting obligations of the service provider to the In-Scope Entity, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements (including the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation) and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
77.j	Contractual phase	the reporting obligations of the service provider to the In-Scope Entity, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements (including the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation) and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;	Functional	Intersects With	Security Compromise Notification Agreements	TPM-21.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5		TPM-05.1
77.k	Contractual phase	whether the service provider shall take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.l	Contractual phase	the requirements to implement and test business contingency plans;	Functional	Intersects With	Provider Contingency Plan	TPM-14.2	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	8		BCD-10.3
77.l	Contractual phase	the requirements to implement and test business contingency plans;	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		TPM-11
77.m	Contractual phase	provisions that ensure that the data that are owned by the In-Scope Entity can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
77.n	Contractual phase	the obligation of the service provider to cooperate with the competent authorities and, where applicable, resolution authorities of the In-Scope Entity, including other persons appointed by them;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.o	Contractual phase	for BRRD institutions, a clear reference to the national resolution authority's powers, especially to Articles 59-47 LFS, 66 and 69 of the BRRD Law, and in particular a description of the 'substantive obligations' of the contract in the sense of the Articles 59-47 LFS and 66 of the BRRD Law;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.p	Contractual phase	the unrestricted right of In-Scope Entities and competent authorities to inspect and audit the service provider, including in case of sub-outsourcing, with regard to, at least, the critical or important outsourced function, as specified in points 88 to 100;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
77.q	Contractual phase	termination rights as specified in points 101 to 103.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
77.q	Contractual phase	termination rights as specified in points 101 to 103.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
78	Sub-outsourcing	The outsourcing agreement shall specify whether or not sub-outsourcing, in particular of critical or important functions, or material parts thereof, is permitted.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
79	Sub-outsourcing	If sub-outsourcing of critical or important functions is permitted, In-Scope Entities shall determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
79	Sub-outsourcing	If sub-outsourcing of critical or important functions is permitted, In-Scope Entities shall determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
80	Sub-outsourcing	If sub-outsourcing of critical or important functions, or material parts thereof, is permitted, the written outsourcing agreement shall:	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
80.a	Sub-outsourcing	specify any types of activities that are excluded from sub-outsourcing;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
80.b	Sub-outsourcing	specify the conditions to be complied with in the case of sub-outsourcing;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
80.c	Sub-outsourcing	specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the In-Scope Entity are continuously met;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
80.d	Sub-outsourcing	require the service provider to obtain prior specific or general written authorisation from the In-Scope Entity before sub-outsourcing data;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
80.e	Sub-outsourcing	include an obligation of the service provider to inform the In-Scope Entity of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set shall allow the In-Scope Entity at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
80.e	Sub-outsourcing	include an obligation of the service provider to inform the In-Scope Entity of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set shall allow the In-Scope Entity at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5		TPM-10
80.f	Sub-outsourcing	ensure, where appropriate, that the In-Scope Entity has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
80.f	Sub-outsourcing	ensure, where appropriate, that the In-Scope Entity has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	3		TPM-10
80.g	Sub-outsourcing	ensure that the In-Scope Entity has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the In-Scope Entity or where the service provider sub-outsources without notifying the In-Scope Entity.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
80.g	Sub-outsourcing	ensure that the In-Scope Entity has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the In-Scope Entity or where the service provider sub-outsources without notifying the In-Scope Entity.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
81	Sub-outsourcing	In-Scope Entities shall agree to sub-outsourcing critical or important functions, or material parts thereof, only if the sub-contractor undertakes to:	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
81.a	Sub-outsourcing	comply with applicable laws, regulatory requirements and contractual obligations; and	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
81.b	Sub-outsourcing	grant the In-Scope Entity and competent authority the same contractual rights of access and audit as those granted by the service provider.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
82	Sub-outsourcing	In-Scope Entities shall ensure that the service provider appropriately oversees the sub-contractors, in line with the policy defined by the In-Scope Entity. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in point 81 above would not be met, the In-Scope Entity shall exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
82	Sub-outsourcing	In-Scope Entities shall ensure that the service provider appropriately oversees the sub-contractors, in line with the policy defined by the In-Scope Entity. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in point 81 above would not be met, the In-Scope Entity shall exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
83	Security of data and systems	The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	3		DCH-01.2
83	Security of data and systems	The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions.	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-25.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.	5		IAC-20.1
83	Security of data and systems	The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5		IAC-21
84	Security of data and systems	In-Scope Entities shall ensure that service providers, where relevant, comply with appropriate ICT security standards.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
84	Security of data and systems	In-Scope Entities shall ensure that service providers, where relevant, comply with appropriate ICT security standards.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
85	Security of data and systems	Where relevant (e.g. in the context of cloud or other ICT outsourcing), In-Scope Entities shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis. Where, in the outsourcing agreement, security measures are made available by the service provider to the In-Scope Entities for personalized selection and configuration (notably for cloud outsourcing), In-Scope Entities shall ensure that proper selection and configuration take place, in line with the In-Scope Entity's security policy and requirements.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-03	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	3		CLD-01.1
85	Security of data and systems	Where relevant (e.g. in the context of cloud or other ICT outsourcing), In-Scope Entities shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis. Where, in the outsourcing agreement, security measures are made available by the service provider to the In-Scope Entities for personalized selection and configuration (notably for cloud outsourcing), In-Scope Entities shall ensure that proper selection and configuration take place, in line with the In-Scope Entity's security policy and requirements.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
85	Security of data and systems	Where relevant (e.g. in the context of cloud or other ICT outsourcing), In-Scope Entities shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis. Where, in the outsourcing agreement, security measures are made available by the service provider to the In-Scope Entities for personalized selection and configuration (notably for cloud outsourcing), In-Scope Entities shall ensure that proper selection and configuration take place, in line with the In-Scope Entity's security policy and requirements.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
86	Security of data and systems	In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, In-Scope Entities shall adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) which shall in particular take into account point 101 c, d and e and information security considerations and comply with the provisions of points 133 to 142.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		CLD-09

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
86	Security of data and systems	In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, In-Scope Entities shall adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) which shall in particular take into account point 101 c, d and e and information security considerations and comply with the provisions of points 133 to 142.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
87	Security of data and systems	Without prejudice to the requirements under GDPR, In-Scope Entities, when outsourcing (in particular to third countries), shall take into account differences in national provisions regarding the protection of data. In-Scope Entities shall ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the In-Scope Entity (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).	Functional	Intersects With	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-22.2	Mechanisms exist to ensure that the requirements for the protection of sensitive and/or regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-13.3
87	Security of data and systems	Without prejudice to the requirements under GDPR, In-Scope Entities, when outsourcing (in particular to third countries), shall take into account differences in national provisions regarding the protection of data. In-Scope Entities shall ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the In-Scope Entity (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5		PRI-07.1
87	Security of data and systems	Without prejudice to the requirements under GDPR, In-Scope Entities, when outsourcing (in particular to third countries), shall take into account differences in national provisions regarding the protection of data. In-Scope Entities shall ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the In-Scope Entity (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
88	Access, information and audit rights	In-Scope Entities shall ensure within the written outsourcing agreement that the internal audit function, the statutory auditor and the competent authority have a guaranteed access to the information relating to the outsourced functions using a risk-based approach in order to enable them to issue a well-founded opinion on the adequacy of the outsourcing. This access implies that they may also verify the relevant data kept by the service provider and, in the cases provided for in the applicable national law, have the power to perform on-site inspections of the service provider. The aforementioned opinion may, where appropriate, be based on the reports of the service provider's external auditor. The written outsourcing agreement shall also provide that the internal control functions have access to any documentation relating to the outsourced functions, at any time and without difficulty, to maintain these functions' continued ability to exercise their controls.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	3		CPL-02.1
88	Access, information and audit rights	In-Scope Entities shall ensure within the written outsourcing agreement that the internal audit function, the statutory auditor and the competent authority have a guaranteed access to the information relating to the outsourced functions using a risk-based approach in order to enable them to issue a well-founded opinion on the adequacy of the outsourcing. This access implies that they may also verify the relevant data kept by the service provider and, in the cases provided for in the applicable national law, have the power to perform on-site inspections of the service provider. The aforementioned opinion may, where appropriate, be based on the reports of the service provider's external auditor. The written outsourcing agreement shall also provide that the internal control functions have access to any documentation relating to the outsourced functions, at any time and without difficulty, to maintain these functions' continued ability to exercise their controls.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
89	Access, information and audit rights	Regardless of the criticality or importance of the outsourced function, the written outsourcing agreement shall refer to the information gathering and investigatory powers of competent authorities under Articles 49, 53 and 59 LFS and Articles 31, 38 and 58-5 LPS and, where applicable, resolution authorities under Article 61(1) BRRD Law with regard to service providers located in a Member State and shall also ensure those rights with regard to service providers located in third countries.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
90	Access, information and audit rights	With regard to the outsourcing of critical or important functions, In-Scope Entities shall ensure within the written outsourcing agreement that the service provider grants them, their statutory auditor and their competent authority, including, where applicable, their resolution authority, and any other person appointed by them or the competent authority or resolution authority, the following:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
90.a	Access, information and audit rights	full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and	Functional	Intersects With	Assessor Access	CPL-10	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	3		CPL-03.3
90.a	Access, information and audit rights	full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
90.b	Access, information and audit rights	unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), including the possibility for the competent authority to communicate any observations made in this context to the In-Scope Entities, to enable them to monitor the outsourcing arrangement and to ensure compliance with the applicable regulatory and contractual requirements;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
91	Access, information and audit rights	For the outsourcing of functions that are not critical or important, In-Scope Entities shall ensure the access and audit rights as set out in point 90 and sub-section 4.3.2.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. In-Scope Entities shall take into account that functions may become critical or important over time.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
91	Access, information and audit rights	For the outsourcing of functions that are not critical or important, In-Scope Entities shall ensure the access and audit rights as set out in point 90 and sub-section 4.3.2.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. In-Scope Entities shall take into account that functions may become critical or important over time.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
91	Access, information and audit rights	For the outsourcing of functions that are not critical or important, In-Scope Entities shall ensure the access and audit rights as set out in point 90 and sub-section 4.3.2.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. In-Scope Entities shall take into account that functions may become critical or important over time.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
92	Access, information and audit rights	In-Scope Entities shall ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, their statutory auditors, competent authorities or third parties appointed by them to exercise these rights.	Functional	Intersects With	Assessor Access	CPL-10	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	3		CPL-03.3
92	Access, information and audit rights	In-Scope Entities shall ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, their statutory auditors, competent authorities or third parties appointed by them to exercise these rights.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
93	Access, information and audit rights	In-Scope Entities shall exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
93	Access, information and audit rights	In-Scope Entities shall exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	Functional	Intersects With	Assessment Methods	CPL-11	Mechanisms exist to define acceptable methods to conduct a cybersecurity and/or data protection assessment.	3		CPL-03.4
93	Access, information and audit rights	In-Scope Entities shall exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
94	Access, information and audit rights	Without prejudice to their final responsibility regarding outsourcing arrangements, In-Scope Entities may use:	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
94.a	Access, information and audit rights	pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-07	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	3		IAO-02.3
94.a	Access, information and audit rights	pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
94.b	Access, information and audit rights	third-party certifications and third-party or internal audit reports, made available by the service provider.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-07	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5		IAO-02.3
94.b	Access, information and audit rights	third-party certifications and third-party or internal audit reports, made available by the service provider.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	8		TPM-05.8
95	Access, information and audit rights	For the outsourcing of critical or important functions, In-Scope Entities shall assess whether third-party certifications and reports as referred to in point 94(b) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
95	Access, information and audit rights	For the outsourcing of critical or important functions, In-Scope Entities shall assess whether third-party certifications and reports as referred to in point 94(b) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
96	Access, information and audit rights	In-Scope Entities shall make use of the method referred to in point 94(b) only if they:	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	3		TPM-05.8
96.a	Access, information and audit rights	are satisfied with the audit plan for the outsourced function;	Functional	Intersects With	Audit Planning Activities	CPL-07.3	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	3		CPL-04
96.a	Access, information and audit rights	are satisfied with the audit plan for the outsourced function;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
96.b	Access, information and audit rights	ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the In-Scope Entity and the compliance with relevant regulatory requirements;	Functional	Intersects With	Compliance Scope	CPL-03	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance	5		CPL-01.2
96.b	Access, information and audit rights	ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the In-Scope Entity and the compliance with relevant regulatory requirements;	Functional	Intersects With	Assessment Boundaries	IAO-03	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	3		IAO-01.1
96.b	Access, information and audit rights	ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the In-Scope Entity and the compliance with relevant regulatory requirements;	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
96.c	Access, information and audit rights	thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
96.c	Access, information and audit rights	thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
96.d	Access, information and audit rights	ensure that key systems and controls are covered in future versions of the certification or audit report;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
96.d	Access, information and audit rights	ensure that key systems and controls are covered in future versions of the certification or audit report;	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
96.e	Access, information and audit rights	are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-09	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5		CPL-01.6
96.e	Access, information and audit rights	are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);	Functional	Intersects With	Assessor Independence	IAO-06	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	3		IAO-02.1
96.f	Access, information and audit rights	are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;	Functional	Intersects With	Assessment Methods	CPL-11	Mechanisms exist to define acceptable methods to conduct a cybersecurity and/or data protection assessment.	3		CPL-03.4
96.f	Access, information and audit rights	are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;	Functional	Intersects With	Technical Verification	IAO-11	Mechanisms exist to perform Control Validation Testing (CVT) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	3		IAO-06
96.f	Access, information and audit rights	are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
96.g	Access, information and audit rights	have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
96.g	Access, information and audit rights	have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	3		TPM-05.8
96.h	Access, information and audit rights	retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
96.h	Access, information and audit rights	retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
97	Access, information and audit rights	In-Scope Entities shall, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
97	Access, information and audit rights	In-Scope Entities shall, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
98	Access, information and audit rights	Before a planned on-site visit, In-Scope Entities, auditors or third parties acting on behalf of the In-Scope Entity or of the competent authority shall provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.	Functional	Intersects With	Audit Planning Activities	CPL-07.3	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5		CPL-04
98	Access, information and audit rights	Before a planned on-site visit, In-Scope Entities, auditors or third parties acting on behalf of the In-Scope Entity or of the competent authority shall provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
99	Access, information and audit rights	When performing audits in multi-client environments, care shall be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
99	Access, information and audit rights	When performing audits in multi-client environments, care shall be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	Functional	Intersects With	Audit Planning Activities	CPL-07.3	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5		CPL-04
100	Access, information and audit rights	Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the In-Scope Entity shall verify that whoever is performing the audit - whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf - has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the In-Scope Entity reviewing third-party certifications or audits carried out by service providers.	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-09	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5		CPL-01.6
100	Access, information and audit rights	Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the In-Scope Entity shall verify that whoever is performing the audit - whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf - has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the In-Scope Entity reviewing third-party certifications or audits carried out by service providers.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
101	Termination rights	The outsourcing agreement shall expressly allow the possibility for the In-Scope Entity to terminate the arrangement in accordance with applicable law, including in the following situations:	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
101.a	Termination rights	where the service provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;	Functional	Intersects With	Non-Conformity Oversight	CPL-06	Mechanisms exist to identify and document instances of non-conformity with statutory, regulatory and/or contractual obligations, in order to develop appropriate risk mitigation actions.	3		CPL-01.1
101.a	Termination rights	where the service provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
101.b	Termination rights	where impediments capable of altering the performance of the outsourced function are identified;	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
101.c	Termination rights	where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	3		TPM-10
101.c	Termination rights	where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
101.d	Termination rights	where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-18	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	3		TPM-09
101.d	Termination rights	where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
101.e	Termination rights	where instructions are given by the In-Scope Entity's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the In-Scope Entity.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
102	Termination rights	The outsourcing agreement shall facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the In-Scope Entity, whenever the continuity or quality of the service provision are likely to be affected. To this end, the written outsourcing agreement shall:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
102.a	Termination rights	clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the In-Scope Entity, including the treatment of data;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
102.b	Termination rights	set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
102.b	Termination rights	set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
102.c	Termination rights	include an obligation of the service provider to support the In-Scope Entity in the orderly transfer of the function in the event of the termination of the outsourcing agreement; and	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
102.d	Termination rights	without prejudice to applicable law, include a commitment for the service provider to erase the data and systems of the In-Scope Entity within a reasonable timeframe when the contract is terminated.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08 DCH-21
102.d	Termination rights	without prejudice to applicable law, include a commitment for the service provider to erase the data and systems of the In-Scope Entity within a reasonable timeframe when the contract is terminated.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
103	Termination rights	The outsourcing arrangement shall not include any termination clause or service termination clause in case of bankruptcy, controlled management, suspension of payments, compositions and arrangements with creditors aimed at preventing bankruptcy or other similar proceedings. In particular, in the context of BRRD institutions, clauses triggering the termination or service termination because of resolution actions, reorganisation measures or a winding-up procedure as required in accordance with the BRRD Law are not allowed.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
104	Oversight of outsourced functions	In-Scope Entities shall monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions, including that the continuity of the services provided under the arrangement and the availability, integrity and security of data and information are ensured. Where the risk, nature or scale of an outsourced function has materially changed, In-Scope Entities shall reassess the criticality or importance	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
104	Oversight of outsourced functions	In-Scope Entities shall monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions, including that the continuity of the services provided under the arrangement and the availability, integrity and security of data and information are ensured. Where the risk, nature or scale of an outsourced function has materially changed, In-Scope Entities shall reassess the criticality or importance	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
105	Oversight of outsourced functions	In-Scope Entities shall apply due skill, care and diligence when planning, implementing, monitoring and managing outsourcing arrangements.	Functional	Intersects With	Defensible Evidence of Due Care	CPL-26.2	Mechanisms exist to produce evidence of due care activities performed that is capable of withstanding external audit or regulatory scrutiny.	3		CPL-13.2
105	Oversight of outsourced functions	In-Scope Entities shall apply due skill, care and diligence when planning, implementing, monitoring and managing outsourcing	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
106	Oversight of outsourced functions	In-Scope Entities shall regularly update their risk assessment in accordance with points 66 to 70 and shall periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
106	Oversight of outsourced functions	In-Scope Entities shall regularly update their risk assessment in accordance with points 66 to 70 and shall periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5		RSK-07
106	Oversight of outsourced functions	In-Scope Entities shall regularly update their risk assessment in accordance with points 66 to 70 and shall periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
107	Oversight of outsourced functions	In-Scope Entities shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account points 66 to 70.	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
107	Oversight of outsourced functions	In-Scope Entities shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account points 66 to 70.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	3		RSK-11
107	Oversight of outsourced functions	In-Scope Entities shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account points 66 to 70.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03
108	Oversight of outsourced functions	In-Scope Entities shall ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced critical or important functions, meet appropriate performance and quality standards in line with their policies by:	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
108.a	Oversight of outsourced functions	ensuring that they receive appropriate reports from service providers;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
108.b	Oversight of outsourced functions	evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-12.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	3		GOV-05.1
108.b	Oversight of outsourced functions	evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
108.c	Oversight of outsourced functions	reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
108.c	Oversight of outsourced functions	reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		TPM-11
109	Oversight of outsourced functions	In-Scope Entities shall take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, In-Scope Entities shall follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, In-Scope Entities shall take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-18	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	8		TPM-09
109	Oversight of outsourced functions	In-Scope Entities shall take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, In-Scope Entities shall follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, In-Scope Entities shall take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7
110	Oversight of outsourced functions	In-Scope Entities shall inform the competent authority with no delay of material changes and/or severe events regarding their outsourcing arrangements that could have a material impact on the continuing provision of their business activities, to allow the competent authority to assess whether regulatory action is needed.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
110	Oversight of outsourced functions	In-Scope Entities shall inform the competent authority with no delay of material changes and/or severe events regarding their outsourcing arrangements that could have a material impact on the continuing provision of their business activities, to allow the competent authority to assess whether regulatory action is needed.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
111	Exit plans	In-Scope Entities shall have a documented exit plan when outsourcing critical or important functions that is in line with their outsourcing policy, exit strategies and business continuity plans, taking into account at least the possibility of:	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5		BCD-01.2
111.a	Exit plans	the termination of outsourcing arrangements;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
111.b	Exit plans	the failure of the service provider;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
111.b	Exit plans	the failure of the service provider;	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	3		TPM-11
111.c	Exit plans	the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
111.c	Exit plans	the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	3		BCD-02.2
111.d	Exit plans	material risks arising for the appropriate and continuous application of the function.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
111.d	Exit plans	material risks arising for the appropriate and continuous application of the function.	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	3		RSK-03
112	Exit plans	In-Scope Entities shall ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they shall:	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5		BCD-01.2
112.a	Exit plans	develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5		BCD-01.2
112.a	Exit plans	develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
112.a	Exit plans	develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
112.b	Exit plans	identify alternative solutions and develop transition plans to enable In-Scope Entities to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the In-Scope Entity or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5		BCD-01.2

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
112.b	Exit plans	identify alternative solutions and develop transition plans to enable In-Scope Entities to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the In-Scope Entity or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	5		BCD-02.2
112.b	Exit plans	identify alternative solutions and develop transition plans to enable In-Scope Entities to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the In-Scope Entity or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.	Functional	Intersects With	Geographic Data Location	DCH-30	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within geographically distributed Technology Assets, Applications and/or Services (TAAS) (physical and virtual).	3		DCH-19
113	Exit plans	When developing exit plans, In-Scope Entities shall:	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
113.a	Exit plans	define the objectives of the exit plan;	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	3		BCD-01.7
113.b	Exit plans	perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
113.b	Exit plans	perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5		RSK-08
113.c	Exit plans	assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	3		BCD-01.7
113.c	Exit plans	assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
113.d	Exit plans	define success criteria for the transition of outsourced functions and data; and	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.5
113.e	Exit plans	define the indicators to be used for the monitoring of the outsourcing arrangement (as outlined under points 104 to 110) including indicators based on unacceptable service levels that shall trigger the exit.	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-12.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	3		GOV-05.2
113.e	Exit plans	define the indicators to be used for the monitoring of the outsourcing arrangement (as outlined under points 104 to 110) including indicators based on unacceptable service levels that shall trigger the exit.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
114	Requirements in the context of ICT outsourcing arrangements	The purpose of this Part is to define specific requirements applicable in the context of ICT outsourcing (cloud and non-cloud), and that shall be complied with in addition to the general requirements laid out in Part I of this circular. The following provisions contribute to the sound and prudent management, the proper organisation of the In-Scope Entities and the preservation of information security of the In-Scope Entities.	Functional	No Relationship	N/A	N/A	N/A	0		
115	Requirements in the context of ICT outsourcing arrangements	The requirements set out in the present Part II do not apply to business process outsourcing (i.e. outsourcing arrangements that are not pure ICT outsourcing) even if the outsourcing arrangements themselves rely on ICT outsourcing i.e. underlying ICT systems form part of this business process outsourcing.	Functional	No Relationship	N/A	N/A	N/A	0		
116	Requirements in the context of ICT outsourcing arrangements	When ICT outsourcing, or at least one of the sub-contractors in case of sub-outsourcing, relies on a cloud computing infrastructure as defined in point 1, the In-Scope Entities shall comply with the requirements of points 114 to 119, as relevant, and Chapter 2 of Part II only. In case of ICT outsourcing arrangements other than those relying on cloud computing infrastructure as defined in point 1, In-Scope Entities shall comply with the requirements of points 114 to 119, as relevant, and Chapter 1 of Part II only.	Functional	No Relationship	N/A	N/A	N/A	0		
117	Requirements in the context of ICT outsourcing arrangements	In case of ICT sub-outsourcing, the requirements of this Part (as applicable in line with point 116) shall apply to the whole outsourcing chain.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
118	Requirements in the context of ICT outsourcing arrangements	In accordance with the principle of proportionality, an In-Scope Entity may, if evidenced by comprehensive and robust conclusions from the assessment of the criticality of functions and the risk analysis, justify not applying the requirements set out in the following points when the ICT outsourcing is not critical or important and is unlikely to become critical or important:	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
118.a	Requirements in the context of ICT outsourcing arrangements	point 103: continuity in case of resolution or reorganisation or another procedure; and	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
118.b	Requirements in the context of ICT outsourcing arrangements	point 112(b): transfer of services where the continuity of the provision of services is threatened.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
119	Requirements in the context of ICT outsourcing arrangements	In-Scope Entities are reminded that for all ICT outsourcing arrangements, they shall:	Functional	No Relationship	N/A	N/A	N/A	0		
119.a	Requirements in the context of ICT outsourcing arrangements	ensure that access to data and systems fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions; and	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-25.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.	5		IAC-20.1
119.a	Requirements in the context of ICT outsourcing arrangements	ensure that access to data and systems fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions; and	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8		IAC-21
119.b	Requirements in the context of ICT outsourcing arrangements	ensure that access to data subject to professional secrecy are granted in compliance with Article 41(2a) LFS or Article 30(2a) LPS where applicable.	Functional	Intersects With	Disclosure of Sensitive / Regulated Data	DCH-08.2	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	5		DCH-03.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
119.b	Requirements in the context of ICT outsourcing arrangements	ensure that access to data subject to professional secrecy are granted in compliance with Article 41(2a) LFS or Article 30(2a) LPS where applicable.	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-25.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.	3		IAC-20.1
120	ICT outsourcing arrangements other than those relying on a cloud computing infrastructure	The requirements of points 59 and 60 apply to ICT outsourcing arrangements concerned by the present chapter.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
121	Requirements applicable to In-Scope Entities other than Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Without prejudice to point 119 above, In-Scope Entities may outsource their ICT system management/operation services:	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
121.a	Requirements applicable to In-Scope Entities other than Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	in Luxembourg, solely to a credit institution or a financial professional holding a support PFS authorisation in accordance with Article 29-3 LFS (IT systems and communication networks operators of the financial sector "OSIRC"); the unique exception allowed under Article 1-1 (2) c) LFS is the recourse to an entity of the group to which the In-Scope Entity belongs and which exclusively deals with group transactions;	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
121.b	Requirements applicable to In-Scope Entities other than Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their	abroad, to any ICT service provider, including an entity of the group to which the In-Scope Entity belongs.	Functional	No Relationship	N/A	N/A	N/A	0		
122	Requirements applicable to In-Scope Entities other than Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	In-Scope Entities may outsource ICT services other than ICT system management/operation services to any ICT service provider, including a group entity providing ICT services or a support PFS. Such outsourcing arrangements must be set up in compliance with the requirements of point 119 above. In particular, if the service provider is not allowed to access to data subject to professional secrecy in compliance with Article 41(2a) LFS or Article 30(2a) LPS where applicable, the service provider may have access to this data only if it is overseen, throughout its mission, by a person of the In-Scope Entity in charge of ICT.	Functional	Intersects With	Disclosure of Sensitive / Regulated Data	DCH-08.2	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	5		DCH-03.1
122	Requirements applicable to In-Scope Entities other than Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	In-Scope Entities may outsource ICT services other than ICT system management/operation services to any ICT service provider, including a group entity providing ICT services or a support PFS. Such outsourcing arrangements must be set up in compliance with the requirements of point 119 above. In particular, if the service provider is not allowed to access to data subject to professional secrecy in compliance with Article 41(2a) LFS or Article 30(2a) LPS where applicable, the service provider may have access to this data only if it is overseen, throughout its mission, by a person of the In-Scope Entity in charge of ICT.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
123	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	For the exclusive purpose of this sub-chapter, the following definitions apply:	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	3		SEA-02.1
123.a	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS: an In-Scope Entity, including its branches, that is authorised to perform OSIRC activities in accordance with Article 29-3 or PSDC activities in accordance with Articles 29-5 or 29-6 LFS;	Functional	No Relationship	N/A	N/A	N/A	0		
123.b	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Own ICT systems systems supporting the support PFS' organisation and administration; they are not proposed as a service to third parties and not used by the services proposed to third parties;	Functional	No Relationship	N/A	N/A	N/A	0		
123.c	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Client ICT systems: systems that fulfill the two following cumulative conditions:	Functional	No Relationship	N/A	N/A	N/A	0		
123.c.i	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	they partially or exclusively support the activities carried out for regulated financial sector clients of the support PFS, irrespective of whether they belong to the client or to the support PFS or where they are located; and	Functional	No Relationship	N/A	N/A	N/A	0		
123.c.ii	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	the support PFS is responsible to its client for their proper functioning.	Functional	No Relationship	N/A	N/A	N/A	0		
124	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Without prejudice to point 119 above, support PFS and their branches authorised as OSIRC in accordance with Article 29-3 LFS may partially outsource their ICT operator services, i.e. some management/operation services of client ICT systems provided that the conditions of points 126 and 127 are fulfilled.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
125	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Without prejudice to point 119 above, support PFS and their branches authorised as PSDC in accordance with Articles 29-5 or 29-6 LFS may partially outsource the management/operation of the ICT systems supporting partially or exclusively the dematerialisation or conservation services they provide to regulated financial sector clients provided that the conditions of points 126 and 127 are fulfilled.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
126	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	The service provider for the outsourcing arrangements referred to in points 124 and 125 above shall be:	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
126.a	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	in Luxembourg, solely a credit institution or an entity that is authorised as support PFS in accordance with Article 29-3 LFS;	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
126.b	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Abroad, any ICT service provider, including an entity of the group to which the support PFS belongs.	Functional	No Relationship	N/A	N/A	N/A	0		
127	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	The outsourcing arrangements referred to in points 124 and 125 above shall be considered as critical or important and are prohibited if they do not comply with the following:	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls;	3		GOV-19.3
127	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	The outsourcing arrangements referred to in points 124 and 125 above shall be considered as critical or important and are prohibited if they do not comply with the following:	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
127.a	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	The service provision is complementary and does not carve out the support PFS (or its branch as relevant) of its substance in line with point 7;	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
127.b	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS and their branches have obtained the prior approval of all their concerned regulated financial sector clients;	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
127.b	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS and their branches have obtained the prior approval of all their concerned regulated financial sector clients;	Functional	Intersects With	Disclosure of Sensitive / Regulated Data	DCH-08.2	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	3		DCH-03.1
127.c	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	If the service provider may have access to data subject to professional secrecy according to Article 41 LFS or Article 30 LPS where applicable, the support PFS and their branches have clearly informed and obtained the prior consent of their regulated financial sector clients;	Functional	Intersects With	Disclosure of Sensitive / Regulated Data	DCH-08.2	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	5		DCH-03.1
127.d	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Each year, the support PFS and their branches must provide the competent authority with their detailed oversight plan and exit plan ensuring compliance with sections 4.3.3 and 4.3.4 of this circular;	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3		BCD-01.2
127.d	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Each year, the support PFS and their branches must provide the competent authority with their detailed oversight plan and exit plan ensuring compliance with sections 4.3.3 and 4.3.4 of this circular;	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
127.e	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS and their branches have obtained the prior approval of the competent authority for such outsourcing using the instructions and, where available, the forms on the CSSF website.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
128	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Without prejudice to points 59, 60 and 119 above, support PFS and their branches may outsource the management/operation services of their own ICT systems:	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
128.a	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	in Luxembourg, solely to a credit institution or an entity that is authorised as support PFS in accordance with Article 29-3 LFS;	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
128.b	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	abroad, to any ICT service provider, including an entity of the group to which the support PFS belongs.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
129	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	The provision of ICT operation services on client ICT systems or on systems supporting PSDC activities, by branches of support PFS to their registered office, are prohibited if they do not comply with the relevant requirements listed in point 127.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
130	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS and their branches acting as OSIRC may, for their services as ICT operators, rely on infrastructures belonging to their group, subject to the condition that the services provided by the group or their sub-contractors, if any, are limited to those requiring a physical presence on these infrastructures. The management of systems containing data and processing to be carried out by the support PFS shall be excluded from such outsourcing. Infrastructure shall mean the IT resources that are necessary to host the systems and data under the management of the OSIRC. In this case, the support PFS shall, in particular, ensure they have permanent control over the actions taken by the group for their account. Where this outsourcing involves the presence on the infrastructure of data subject to the professional secrecy according to Article 41 LFS or Article 30 LPS, where applicable, the support PFS shall obtain the approval of the regulated financial sector clients before outsourcing.	Functional	Intersects With	Disclosure of Sensitive / Regulated Data	DCH-08.2	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	3		DCH-03.1
130	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS and their branches acting as OSIRC may, for their services as ICT operators, rely on infrastructures belonging to their group, subject to the condition that the services provided by the group or their sub-contractors, if any, are limited to those requiring a physical presence on these infrastructures. The management of systems containing data and processing to be carried out by the support PFS shall be excluded from such outsourcing. Infrastructure shall mean the IT resources that are necessary to host the systems and data under the management of the OSIRC. In this case, the support PFS shall, in particular, ensure they have permanent control over the actions taken by the group for their account. Where this outsourcing involves the presence on the infrastructure of data subject to the professional secrecy according to Article 41 LFS or Article 30 LPS, where applicable, the support PFS shall obtain the approval of the regulated financial sector clients before outsourcing.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
130	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS and their branches acting as OSIRC may, for their services as ICT operators, rely on infrastructures belonging to their group, subject to the condition that the services provided by the group or their sub-contractors, if any, are limited to those requiring a physical presence on these infrastructures. The management of systems containing data and processing to be carried out by the support PFS shall be excluded from such outsourcing. Infrastructure shall mean the IT resources that are necessary to host the systems and data under the management of the OSIRC. In this case, the support PFS shall, in particular, ensure they have permanent control over the actions taken by the group for their account. Where this outsourcing involves the presence on the infrastructure of data subject to the professional secrecy according to Article 41 LFS or Article 30 LPS, where applicable, the support PFS shall obtain the approval of the regulated financial sector clients before outsourcing.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
131	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Branches of support PFS may propose services relying on an infrastructure established in the country in which they are established ("host country") to their regulated financial clients in the host country. This infrastructure may be outsourced to a local service provider, subject to the condition that the services provided by this service provider and its sub-contractors, if any, are limited to those requiring a physical presence on these infrastructures and excluding any management of systems containing data and processing to be carried out by the support PFS or its branch. The branch shall apply the principles laid down in this circular, and the registered office in Luxembourg shall keep the appropriate oversight of the services provided by its branch. The branches shall obtain approval for this local outsourcing from their regulated financial sector clients	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-04
131	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Branches of support PFS may propose services relying on an infrastructure established in the country in which they are established ("host country") to their regulated financial clients in the host country. This infrastructure may be outsourced to a local service provider, subject to the condition that the services provided by this service provider and its sub-contractors, if any, are limited to those requiring a physical presence on these infrastructures and excluding any management of systems containing data and processing to be carried out by the support PFS or its branch. The branch shall apply the principles laid down in this circular, and the registered office in Luxembourg shall keep the appropriate oversight of the services provided by its branch. The branches shall obtain approval for this local outsourcing from their regulated financial sector clients	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
132	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS may outsource any ICT services other than those covered by points 124 to 131 above to any ICT service provider, including a group entity providing ICT services or a support PFS. Such outsourcing arrangements must be set up in compliance with the requirements of point 119 above. In particular, if the service provider is not allowed to access to data subject to professional secrecy in compliance with Article 41 LFS or Article 30 LPS where applicable, the service provider may have access to this data only if it is overseen, throughout its mission, by a person of the Support PFS in charge of ICT.	Functional	Intersects With	Disclosure of Sensitive / Regulated Data	DCH-08.2	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	5		DCH-03.1
132	Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad	Support PFS may outsource any ICT services other than those covered by points 124 to 131 above to any ICT service provider, including a group entity providing ICT services or a support PFS. Such outsourcing arrangements must be set up in compliance with the requirements of point 119 above. In particular, if the service provider is not allowed to access to data subject to professional secrecy in compliance with Article 41 LFS or Article 30 LPS where applicable, the service provider may have access to this data only if it is overseen, throughout its mission, by a person of the Support PFS in charge of ICT.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
133	ICT outsourcing arrangements relying on a cloud computing infrastructure	This chapter provides additional specific requirements to comply with in case of ICT outsourcing relying on a cloud computing infrastructure (hereafter also "cloud computing solution"). The use of a private cloud without outsourcing is thus excluded from the scope of this chapter.	Functional	No Relationship	N/A	N/A	N/A	0		
134	Specific terminology	For the purposes of this chapter and in addition to definitions provided in point 1, the following definitions shall apply: 1) Client interface the software layer made available by the cloud computing service provider to the In-Scope Entity allowing the latter to manage its cloud computing resources. 2) Cloud computing resource any computing capabilities (e.g. server, storage, network, etc.) provided by a cloud computing service provider. 3) Cloud computing service any firm proposing cloud services within the meaning of the provider definition of this Chapter 2. 4) In-Scope Entity an In-Scope Entity as defined in point 2, is consuming Cloud computing resources for the purpose of carrying out its activities. 5) Multi-tenant a physical or logical infrastructure serving several (In-Scope) Entities through shared cloud computing resources and by means of a standardised model. 6) Resource operation managing cloud computing resources made available through the client interface. By extension, "resource operator" shall mean the natural or legal person that uses the client	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
135	Definition of "cloud computing"	Cloud computing is a model composed of the following five essential characteristics:	Functional	No Relationship	N/A	N/A	N/A	0		
135.a	Definition of "cloud computing"	On-demand self-service: An In-Scope Entity can unilaterally provide computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with the cloud computing service provider.	Functional	No Relationship	N/A	N/A	N/A	0		
135.b	Definition of "cloud computing"	Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin (e.g. browsers) or thick client (e.g. specific applications) platforms (e.g. mobile phones, tablets, laptops and workstations).	Functional	No Relationship	N/A	N/A	N/A	0		
135.c	Definition of "cloud computing"	Resource pooling: The cloud computing service provider's computing resources are pooled to serve multiple (In-Scope) Entities using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to In-Scope Entity demand. There is a sense of location independence in that the In-Scope Entity generally has no control or knowledge over the exact location of the provided resources, but may be able to specify the location at a higher level of abstraction (e.g. country, region or data centre). Examples of resources include storage, processing, memory and network bandwidth.	Functional	No Relationship	N/A	N/A	N/A	0		
135.d	Definition of "cloud computing"	Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the In-Scope Entity, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.	Functional	No Relationship	N/A	N/A	N/A	0		
135.e	Definition of "cloud computing"	Measured service: Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and the In-Scope Entity of the utilised service.	Functional	No Relationship	N/A	N/A	N/A	0		
136	Conditions of application of Chapter 2	An outsourcing is considered as "outsourcing to a cloud computing infrastructure" within the meaning of this circular and governed by the requirements of this Chapter 2 if the five essential characteristics defined in point 135 and both of the following specific requirements are fulfilled:	Functional	No Relationship	N/A	N/A	N/A	0		
136.a	Conditions of application of Chapter 2	Under no circumstances may staff employed by the cloud computing service provider access data and systems that an In-Scope Entity owns on a cloud computing infrastructure without prior and explicit agreement of the In-Scope Entity and without monitoring mechanism available to the In-Scope Entity to control the accesses. These accesses must remain exceptional. Nevertheless, access may be necessary under a legal requirement or in an extreme emergency following a critical incident affecting part of or all the (In-Scope) Entities of the cloud computing service provider. All accesses of the cloud computing service provider must be restricted and subject to preventive and detective measures in line with sound security practices and audited at least annually.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
136.a	Conditions of application of Chapter 2	Under no circumstances may staff employed by the cloud computing service provider access data and systems that an In-Scope Entity owns on a cloud computing infrastructure without prior and explicit agreement of the In-Scope Entity and without monitoring mechanism available to the In-Scope Entity to control the accesses. These accesses must remain exceptional. Nevertheless, access may be necessary under a legal requirement or in an extreme emergency following a critical incident affecting part of or all the (In-Scope) Entities of the cloud computing service provider. All accesses of the cloud computing service provider must be restricted and subject to preventive and detective measures in line with sound security practices and audited at least annually.	Functional	Intersects With	Privileged User Oversight	MON-14.2	Mechanisms exist to implement enhanced activity monitoring for privileged users.	3		MON-01.15
136.a	Conditions of application of Chapter 2	Under no circumstances may staff employed by the cloud computing service provider access data and systems that an In-Scope Entity owns on a cloud computing infrastructure without prior and explicit agreement of the In-Scope Entity and without monitoring mechanism available to the In-Scope Entity to control the accesses. These accesses must remain exceptional. Nevertheless, access may be necessary under a legal requirement or in an extreme emergency following a critical incident affecting part of or all the (In-Scope) Entities of the cloud computing service provider. All accesses of the cloud computing service provider must be restricted and subject to preventive and detective measures in line with sound security practices and audited at least annually.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
136.b	Conditions of application of Chapter 2	The cloud service provision does not entail any manual interaction by the cloud computing service provider as regards the day-to-day management of the cloud computing resources used by the In-Scope Entity (e.g. provisioning, configuration or release of cloud computing resources). Thus, the resource operator alone (i.e. either the In-Scope Entity or a third party other than the cloud computing service provider) shall manage its ICT environment hosted on the cloud computing infrastructure. However, the cloud computing service provider may intervene manually:	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	3		CLD-06.1
136.b.i	Conditions of application of Chapter 2	for global management of ICT systems supporting the cloud computing infrastructure (e.g. maintenance of physical equipment, deployment of new solutions non specific to the In-Scope Entity); or	Functional	No Relationship	N/A	N/A	N/A	0		
136.b.ii	Conditions of application of Chapter 2	within the context of a specific request by the In-Scope Entity (e.g. provisioning of a cloud computing resource that is missing in the catalogue proposed by the cloud computing service provider or performing insufficiently).	Functional	No Relationship	N/A	N/A	N/A	0		
137	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	In accordance with the principle of proportionality, the In-Scope Entity may, if evidenced by comprehensive and robust conclusions from the assessment of the criticality and importance of functions and the risk analysis, justify not to apply the requirements set out in the following points of this circular when the activities outsourced to a cloud computing infrastructure are not related to a critical or important function and are unlikely to become critical or important:	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
137.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	point 142 c.: notification by the cloud computing service provider in case of change of functionalities;	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	3		TPM-10
137.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	point 142 d.: notification by the resource operator in case of change of functionalities.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	3		TPM-10
138	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity may outsource the "resource operation" as defined in point 134 to a third party when this third party falls under one of the following two circumstances:	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
138.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The third-party is authorised as OSIRC under Article 29-3 LFS. The support PSF shall also comply with the requirements of this chapter where the operation of resources is carried out for an entity which is not a regulated financial sector client.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
138.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The third-party is not authorised as OSIRC under Article 29-3 LFS, either because it is located abroad, or because it is a Luxembourg-based entity of the group to which the In-Scope Entity belongs which provides operating services exclusively within the group as stated under the Article 1-1(2)c LFS. In such a case, in addition to complying with the requirements set out in this circular, the In-Scope Entity shall perform a prior thorough risk analysis of the activities of the resource operator, notably by verifying that the following points have been correctly addressed:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
138.b.i	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the roles and responsibilities defined between the resource operator and the cloud computing service provider;	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	5		CLD-06.1
138.b.ii	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the management of the isolation of multi-tenant environments;	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
138.b.iii	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the indicators collected by the resource operator to monitor the systems and data on the cloud computing infrastructure;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
138.b.iv	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the technical and organisational security measures implemented to access the client interfaces in order to manage the cloud computing resources, including the management of client interface access;	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	3		IAC-01
138.b.v	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the consistency of the operations and security policies defined by the resource operator with the configurations of the cloud computing resources and the planned security measures;	Functional	Intersects With	Configuration Management Program	CFG-02	Mechanisms exist to facilitate the implementation of configuration management controls.	3		CFG-01
138.b.vi	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the competences of the operators (e.g. certifications, technical training);	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
138.b.vii	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the review of the audit reports of the cloud computing service provider by the resource operator;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
138.b.viii	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the competent authority's and the In-Scope Entity's right to audit the resource operator (in line with the requirements under points 88 to 100).	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
139	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	It shall be noted that an In-Scope Entity relying on a service provider that cumulates the activities of cloud computing service provider and resource operator is subject to the requirements of this Chapter 2 provided that both activities are properly segregated (i.e. so that staff exercising the cloud computing service provider function cannot access data and thereby continues to fulfil the definition of cloud computing within the meaning of this chapter). The same applies where the service provider cumulating both functions is authorised under Article 29-3 LFS. If this segregation requirement cannot be fulfilled, the outsourcing is not considered as an outsourcing to a cloud computing infrastructure within the meaning of this chapter but as a traditional ICT outsourcing; in such a case only the requirements of Chapter 1 of	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
140	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Cloud Officer:	Functional	No Relationship	N/A	N/A	N/A	0		
140.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The resource operator shall designate among its employees one person, the "cloud officer", who shall be responsible for the use of cloud services and shall guarantee the competences of the staff managing cloud computing resources (cf. point 142a). The resource operator shall assign the function of "cloud officer" to a qualified person that masters the challenges of outsourcing to a cloud computing infrastructure. This function may be taken up by persons that already cumulate other functions within the ICT department.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		GOV-04
140.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The resource operator shall designate among its employees one person, the "cloud officer", who shall be responsible for the use of cloud services and shall guarantee the competences of the staff managing cloud computing resources (cf. point 142a). The resource operator shall assign the function of "cloud officer" to a qualified person that masters the challenges of outsourcing to a cloud computing infrastructure. This function may be taken up by persons that already cumulate other functions within the ICT department.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
140.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	If resource operation is performed by the In-Scope Entity, the "cloud officer" may cumulate the responsibility for the outsourcing relationship management. If the In-Scope Entity relies on a third party for cloud computing resource operation, the In-Scope Entity must know the name of the "cloud officer" of the resource operator.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
141	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Necessity to inform the competent authority:	Functional	No Relationship	N/A	N/A	N/A	0		
141.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The notification requirements of points 59 and 60 also apply to cloud computing outsourcing arrangements. In the particular case where an entity authorised under Article 29-3 LFS acts as an intermediary and not as a resource operator between an In-Scope Entity and a cloud computing service provider, the In-Scope Entity shall submit a notification at least three (3) months before the planned outsourcing is effectively implemented for the outsourcing of critical or important functions to the cloud computing service provider.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
141.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Any entity authorised as OSIRC under Article 29-3 LFS shall request authorisation from the competent authority before marketing in the following cases:	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
141.b.i	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the entity intends to act as a resource operator for its regulated financial sector clients;	Functional	No Relationship	N/A	N/A	N/A	0		
141.b.ii	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the entity intends to provide a cloud computing infrastructure to its regulated financial sector clients, acting thus as a cloud computing service provider;	Functional	No Relationship	N/A	N/A	N/A	0		
141.b.iii	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	the entity intends to provide a cloud computing solution to its regulated financial sector clients by relying on one or more cloud computing infrastructures. This entity acts then as a sub-outsourcing cloud computing service provider.	Functional	No Relationship	N/A	N/A	N/A	0		
141.c	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Without prejudice to point 119, support PFS and their branches authorised as OSIRC under Article 29-3 LFS may partially outsource their resource operator services only under the conditions that compliance with point 126 and the requirements listed under point 127 are fulfilled. For the sake of clarity, a prior approval by the competent authority is therefore required as indicated in point 127 e. Point 129 also applies mutatis mutandis for the provision of resource operator services.	Functional	Intersects With	Security, Compliance & Resilience Outsourcing Limitations	TPM-05	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	3		GOV-19.3
142	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Management of outsourcing risks:	Functional	No Relationship	N/A	N/A	N/A	0		
142.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	In line with point 35, the resource operator shall retain the necessary expertise to effectively monitor the outsourced services or functions on a cloud computing infrastructure and manage the risks associated with the outsourcing. Moreover, the resource operator shall ensure that staff in charge of cloud computing resources management, including the "cloud officer", have sufficient competences to take on their functions based on appropriate training in management and security of cloud computing resources that are specific to the cloud computing service provider;	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
142.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	In line with point 35, the resource operator shall retain the necessary expertise to effectively monitor the outsourced services or functions on a cloud computing infrastructure and manage the risks associated with the outsourcing. Moreover, the resource operator shall ensure that staff in charge of cloud computing resources management, including the "cloud officer", have sufficient competences to take on their functions based on appropriate training in management and security of cloud computing resources that are specific to the cloud computing service provider;	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03
142.a	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	In line with point 35, the resource operator shall retain the necessary expertise to effectively monitor the outsourced services or functions on a cloud computing infrastructure and manage the risks associated with the outsourcing. Moreover, the resource operator shall ensure that staff in charge of cloud computing resources management, including the "cloud officer", have sufficient competences to take on their functions based on appropriate training in management and security of cloud computing resources that are specific to the cloud computing service provider;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
142.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	As set out in points 66 to 70, a risk assessment of outsourcing arrangements shall be carried out by the In-Scope Entity. The risks specific to the use of cloud computing technologies shall also be part of this assessment and encompass, e.g.: isolation failure in multi-tenant environments, the various legislations that are applicable (country where data are stored and country where the cloud computing service provider is established), interception of data-in-transit, failure of telecommunications (e.g. Internet connection), the use of the cloud as "shadow IT", the lack of systems portability once they have been deployed on a cloud computing infrastructure or the failure of continuity of cloud computing services;	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
142.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	As set out in points 66 to 70, a risk assessment of outsourcing arrangements shall be carried out by the In-Scope Entity. The risks specific to the use of cloud computing technologies shall also be part of this assessment and encompass, e.g.: isolation failure in multi-tenant environments, the various legislations that are applicable (country where data are stored and country where the cloud computing service provider is established), interception of data-in-transit, failure of telecommunications (e.g. Internet connection), the use of the cloud as "shadow IT", the lack of systems portability once they have been deployed on a cloud computing infrastructure or the failure of continuity of cloud computing services;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
142.b	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	As set out in points 66 to 70, a risk assessment of outsourcing arrangements shall be carried out by the In-Scope Entity. The risks specific to the use of cloud computing technologies shall also be part of this assessment and encompass, e.g.: isolation failure in multi-tenant environments, the various legislations that are applicable (country where data are stored and country where the cloud computing service provider is established), interception of data-in-transit, failure of telecommunications (e.g. Internet connection), the use of the cloud as "shadow IT", the lack of systems portability once they have been deployed on a cloud computing infrastructure or the failure of continuity of cloud computing services;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
142.c	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Any change in the application functionality by the cloud computing service provider - other than the changes relating to corrective maintenance - shall be communicated prior to its implementation to the resource operator who shall inform the In-Scope Entity, so that they may take the necessary measures in case of material change or discontinuity;	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	3		CHG-05
142.c	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Any change in the application functionality by the cloud computing service provider - other than the changes relating to corrective maintenance - shall be communicated prior to its implementation to the resource operator who shall inform the In-Scope Entity, so that they may take the necessary measures in case of material change or discontinuity;	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5		TPM-10
142.d	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Any change in the application functionality managed by the resource operator - other than the changes relating to corrective maintenance - shall be communicated to the In-Scope Entity, prior to its implementation, so that the latter may take the necessary measures in case of material change or discontinuity;	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	3		CHG-05
142.d	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	Any change in the application functionality managed by the resource operator - other than the changes relating to corrective maintenance - shall be communicated to the In-Scope Entity, prior to its implementation, so that the latter may take the necessary measures in case of material change or discontinuity;	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5		TPM-10
142.e	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity and the resource operator shall have full awareness of the continuity and security elements remaining under their responsibilities when using a cloud computing solution;	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	8		CLD-06.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 22/806 (as amended by Circulars CSSF 25/883 and 26/915) - Outsourcing**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-22-806/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-22-806.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
142.e	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity and the resource operator shall have full awareness of the continuity and security elements remaining under their responsibilities when using a cloud computing solution;	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5		TPM-05.4
142.f	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity shall understand and the resource operator shall control the risks linked to a cloud computing infrastructure;	Functional	Intersects With	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5		CLD-01
142.f	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity shall understand and the resource operator shall control the risks linked to a cloud computing infrastructure;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
142.g	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity and the resource operator shall know at any time where their data and systems are located globally, be it production environments or replications or backups.	Functional	Intersects With	Logical Data Location	DCH-29	Mechanisms exist to identify and document the logical location of data and the specific Technology Assets, Applications and/or Services (TAAS) on which the data resides.	3		DCH-24
142.g	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity and the resource operator shall know at any time where their data and systems are located globally, be it production environments or replications or backups.	Functional	Intersects With	Geographic Data Location	DCH-30	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within geographically distributed Technology Assets, Applications and/or Services (TAAS) (physical and virtual).	8		DCH-19
142.g	Requirements to be observed with respect to outsourcing to a cloud computing infrastructure	The In-Scope Entity and the resource operator shall know at any time where their data and systems are located globally, be it production environments or replications or backups.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		CLD-09
143	Date of application	This circular is applicable from 30 June 2022 to all outsourcing arrangements entered into, reviewed or amended on or after this date.	Functional	No Relationship	N/A	N/A	N/A	0		
144	Date of application	In-Scope Entities shall review and amend existing outsourcing arrangements with a view to ensuring that they are compliant with this circular.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
145	Date of application	In-Scope Entities shall complete the documentation of all existing outsourcing arrangements in line with this circular following the first renewal date of each existing outsourcing arrangement, but by no later than 31 December 2022. Where the In-Scope Entities assess that the review and amendment of outsourcing arrangements of critical or important functions existing prior to 30 June 2022 will not be finalised by 31 December 2022, they shall inform their competent authority in a timely manner of that fact, including the measures planned to complete the review or the possible exit strategy. Claude WAMPACH Marco ZWICK Jean-Pierre FABER Director Director Director Françoise KAUTHEN Claude MARX Director Director General Annex List of implemented ESA Guidelines This circular implements: the revised EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02); the ESMA Guidelines on outsourcing to cloud service providers (ESMA50-164-4285, the ESMA Cloud Guidelines) previously implemented by Circular CSSF 21/777 amending Circular CSSF 17/654. The above-mentioned guidelines are available on the websites of the EBA (www.eba.europa.eu) and ESMA (www.esma.europa.eu).	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1