Cybersecurity & Data Privacy Risk Management Model (C|P-RMM)

version 2024.1

www.ComplianceForge.com

www.SecureControlsFramework.com

START HERE

1 Identify one or more risk management principles that will form the basis of how the entity approaches its risk management processes. The alignment with risk management principles must support the entity's policies and standards for risk management objectives.

"NIST-aligned" principles		"ISO-aligned" principles		"COSO-aligned" principles		"OMB-aligned" principles
NIST SP 800-37 NIST SP 800-39 NIST IR 8286	OR	ISO 31010	OR	COSO 2019	OR	OMB A-123

2 Identify, implement and document critical dependencies that are necessary to legitimately identify, assess and manage risk.

2a Establish risk management dependencies

- Define the "acceptable risk" threshold for the entity
- Define risk occurrence likelihoods
- Define risk impact effects
- Identify the risk authority for various levels of management
- Define risk levels
- Establish a Plan of Action & Milestones (POA&M) or risk register

2b Establish technology dependencies that affect risk management decisions

- Accurate & current hardware & software inventories
- Accurate & current network diagrams
- Accurate & current Data Flow Diagrams (DFD)
- Understanding of technology dependencies that affect operations
- Consistent application of security & privacy controls
- Results from vulnerability assessments

2c Establish business dependencies that affect risk management decisions

- Establish a data classification scheme, including what constitutes the "crown jewels" for data protection requirements
- Enforce policies and standards across the entity
- Define "what right looks like" by identifying a target maturity level for security & privacy
- Enforce the documentation of business practices
- Implement third-party governance as part of a Supply Chain Risk Management (SCRM) program
- Assign competent & trained personnel to the roles that make risk management decisions

3 Formalize Risk Practices

Document a formal **Risk Management Program (RMP)** that supports the entity's policies & standards. The RMP is meant to document the program-level guidance that defines the "*who, what, why, when & how*" about the entity's specific risk management practices.

4 Develop a **RISK CATALOG** that identifies the possible risks that affect the entity.

5 Develop a **THREAT CATALOG** that identifies possible natural and man-made threats that affect the entity's security & privacy controls.

6 Develop a **CONTROLS CATALOG** that addresses the entity's applicable statutory, regulatory and contractual obligations. Risks must map to the entity's security & privacy controls. Ideally, the controls are weighted since not all security & privacy controls are equal.

SCF SECURE CONTROLS FRAMEWORK

SCF has built-In Control Weighting Values [1-10] , the Security & Privacy Capability Maturity Model (C|P-CMM) and the SCF controls written in question format.

7 Per the entity's target **Capability Maturity Model (CMM)** target, identify "what right looks like" for each security & privacy control.

** Assessing risks in the context of the C|P-RMM applies to various assessment scenarios:
- Cybersecurity Risk Assessment
- Third-Party Risk Assessment
- Data Protection Impact Assessment (DPIA)
- Business Impact Assessment (BIA)
- Privacy Impact Assessment (PIA)

8 Perform Risk Assessments **

Risk Assessment Rigor
- Level 1 - Basic (Minimum Assurance)
- Level 2 - Focused (Minimum Assurance)
- Level 3 - Comprehensive (Minimum Assurance)

9 Establish the context of the **Security & Privacy Risk Environment (SPRE)**. The SPRE is the overall operating environment that is in scope for the risk assessment. This is where the threats, risks and vulnerabilities affect the entity's protection measures. This can be addressed through a well-documented **System Security & Privacy Plan (SSPP)**.

Category	System Security & Privacy Plan (SSPP) Components
Background Information	General description & purpose
	Applicable statutory, regulatory & contractual requirements
	Applicable contracts
	Stakeholders (internal & external)
	Unique data protection considerations
System Environment Description	Hardware & software in use
	Geo-location considerations (storage & processing)
	Identity & Access Management (IAM)
	Network boundaries
	Supply chain overview
	Ongoing maintenance & support plan

10 From the applicable security & privacy controls, evaluate those controls based on the entity's **THREAT CATALOG** to identify current or potential control deficiencies. Utilize the **RISK CATALOG** to identify the applicable risks from the control deficiencies.

Findings
- Satisfactory
- Not Applicable
- Alternative
- Deficient

11 Utilize entity-accepted methods to assess the control in the most objective method possible.

Assessment Methods
- Method 1 **Qualitative**
- Method 2 **Semi-Qualitative**
- Method 3 **Quantitative**

SP-RMM Risk Matrix

Impact Effect (IE) \ Occurrence Likelihood (OL)	Remote [< 1% chance of occurrence]	Highly Unlikely [1% to 10% chance of occurrence]	Unlikely [10% to 25% chance of	Possible [25% to 70% chance of	Likely [70% to 99% chance of	Almost Certain [> 99% chance of occurrence]
Catastrophic						EXTREME RISK
Critical					SEVERE RISK	
Major				HIGH RISK		
Moderate			MODERATE RISK			
Minor		LOW RISK				
Insignificant						

Impact Effect (IE)

Catastrophic	Critical, long-term damage or service impact. Financial and reputational damage could be enough to ruin the business.
Critical	Critical, short-term damage or service impact. Financial and reputational damage could create noticeable loss of market share.
Major	Major damage or service impact. Extensive reputational and financial impact, but not enough to ruin the business.
Moderate	Noticeable damage or service impact. Harmful reputational and financial impact, but not enough to ruin the business.
Minor	Localized or minimal damage or service impact. Minor reputational and financial impact.
Insignificant	Little to no damage or service impact. No reputational or financial impact.

Occurrence Likelihood (OL)

Almost Certain	Virtual certainty the event will occur at some time, under normal business conditions, that can be quantified as greater than a 99% chance of occurrence.
Likely	Likely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 70%-99% chance of occurrence.
Possible	Reasonable to expect the event could occur at some time, under normal business conditions, that can be quantified as between a 25%-70% chance of occurrence.
Unlikely	Unlikely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 10%-25% chance of occurrence.
Highly Unlikely	Highly-unlikely event that can be quantified as between a 1%-10% chance of occurrence.
Remote	Theoretically possible. The likelihood of occurring can be quantified as less than a 1% chance of occurrence.

NVD Vulnerability Severity Ratings CVSS 3.0 Ratings***

Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None	0.0

*** Where feasible, the NVD Vulnerability Severity Ratings should be leveraged to provide objectivity when evaluating a technical risk. The CVSS 3.0 rating can be leveraged to determine an appropriate Risk Impact Effect that is specific to the entity's use of the technology in question.

12 Prioritize and document the identified risks.

- Priority 1 **Emergency**
- Priority 2 **Elevated**
- Priority 3 **Standard**

- Risk Assessment Report
- Plan of Action & Milestones (POA&M)
- Risk Register
- System Security & Privacy Plan (SSPP)

- Low
- Moderate
- High
- Severe
- Extreme

13 Calculate Risk ***

***CALCULATING INHERENT RISK**:
The Occurrence Likelihood (OL), in combination with the Impact Effect (IE) will provide the "inherent risk" score. This is considered a raw or unmitigated risk score. It is important to note that inherent risk does not take into account any control weighting, the maturity of implemented controls or any other mitigating factors.

CALCULATING RESIDUAL RISK:
To understand the "residual risk" that takes into account control weighting, the maturity of implemented controls and other mitigating factor, it requires expanding upon inherent risk calculations. To identify the residual risk score, Occurrence Likelihood (OL) is calculated by Risk Impact Effect (IE), Control Weighting (CW), Maturity Level (ML) and Mitigating Factors (MF).

14 Report on Conformity (ROC)

- Conforms
- Significant Deficiency
- Material Weakness

- Tier 1 Management **Line Management**
- Tier 2 Management **Senior Management**
- Tier 3 Management **Executive Management**
- Tier 4 Management **Board of Directors**

15 Identify Appropriate Management Audience

16 Management Determines Risk Treatment

- Risk Treatment Option # 1 **Reduce the risk to an acceptable level**
- Risk Treatment Option # 2 **Avoid the risk**
- Risk Treatment Option # 3 **Transfer the risk to another party**
- Risk Treatment Option # 4 **Accept the risk**

- Risk Status 1 **Open (unacceptable risk)**
- Risk Status 2 **Open (acceptable risk)**
- Risk Status 3 **Closed**

17 Implement risk treatment options. Document risk status through remediation.

[continuous risk monitoring & assessments]

Definition of "risk" in the context of the C|P-RMM:
noun A situation where someone or something valued is exposed to danger, harm or loss.*
verb To expose someone or something valued to danger, harm or loss.

* Danger: state of possibly suffering harm or injury
* Harm: material / physical damage
* Loss: destruction, deprivation or inability to use

Definition of "threat" in the context of the C|P-RMM:
noun A person or thing likely to cause damage or danger.
verb To indicate impending damage or danger.

Risk Grouping	Risk #	Risk
Access Control	R-AC-1	Inability to maintain individual accountability
	R-AC-2	Improper assignment of privileged functions
	R-AC-3	Privilege escalation
	R-AC-4	Unauthorized access
Asset Management	R-AM-1	Lost, damaged or stolen asset(s)
	R-AM-2	Loss of integrity through unauthorized changes
	R-AM-3	Emergent properties and/or unintended consequences
Business Continuity	R-BC-1	Business interruption
	R-BC-2	Data loss / corruption
	R-BC-3	Reduction in productivity
	R-BC-4	Information loss / corruption or system compromise due to technical attack
	R-BC-5	Information loss / corruption or system compromise due to non-technical attack
Exposure	R-EX-1	Loss of revenue
	R-EX-2	Cancelled contract
	R-EX-3	Diminished competitive advantage
	R-EX-4	Diminished reputation
	R-EX-5	Fines and judgements
	R-EX-6	Unmitigated vulnerabilities
	R-EX-7	System compromise
Governance	R-GV-1	Inability to support business processes
	R-GV-2	Incorrect controls scoping
	R-GV-3	Lack of roles & responsibilities
	R-GV-4	Inadequate internal practices
	R-GV-5	Inadequate third-party practices
	R-GV-6	Lack of oversight of internal controls
	R-GV-7	Lack of oversight of third-party controls
	R-GV-8	Illegal content or abusive action
Incident Response	R-IR-1	Inability to investigate / prosecute incidents
	R-IR-2	Improper response to incidents
	R-IR-3	Ineffective remediation actions
	R-IR-4	Expense associated with managing a loss event
Situational Awareness	R-SA-1	Inability to maintain situational awareness
	R-SA-2	Lack of a security-minded workforce

Threat Grouping	Threat #	Threat*
Natural Threat	NT-1	Drought & Water Shortage
	NT-2	Earthquakes
	NT-3	Fire & Wildfires
	NT-4	Floods
	NT-5	Hurricanes & Tropical Storms
	NT-6	Landslides & Debris Flow
	NT-7	Pandemic (Disease) Outbreaks
	NT-8	Severe Weather
	NT-9	Space Weather
	NT-10	Thunderstorms & Lightning
	NT-11	Tornadoes
	NT-12	Tsunamis
	NT-13	Volcanoes
	NT-14	Winter Storms & Extreme Cold
Man-Made Threat	MT-1	Civil or Political Unrest
	MT-2	Hacking & Other Cybersecurity Crimes
	MT-3	Hazardous Materials Emergencies
	MT-4	Nuclear, Biological and Chemical (NBC) Weapons
	MT-5	Physical Crime
	MT-6	Terrorism & Armed Attacks
	MT-7	Utility Service Disruption
	MT-8	Dysfunctional Management Practices
	MT-9	Human Error
	MT-10	Technical / Mechanical Failure
	MT-11	Statutory / Regulatory / Contractual Obligation
	MT-12	Redundant, Obsolete/Outdated, Toxic or Trivial (ROT) Data
	MT-13	Artificial Intelligence & Autonomous Technologies (AAT)

Capability Maturity Model

Define "what right looks like" by identifying a target maturity level. This can be done through the **Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM)**.

The criteria of the C|P-CMM can be used for both planning purposes and as a benchmark to assess against.

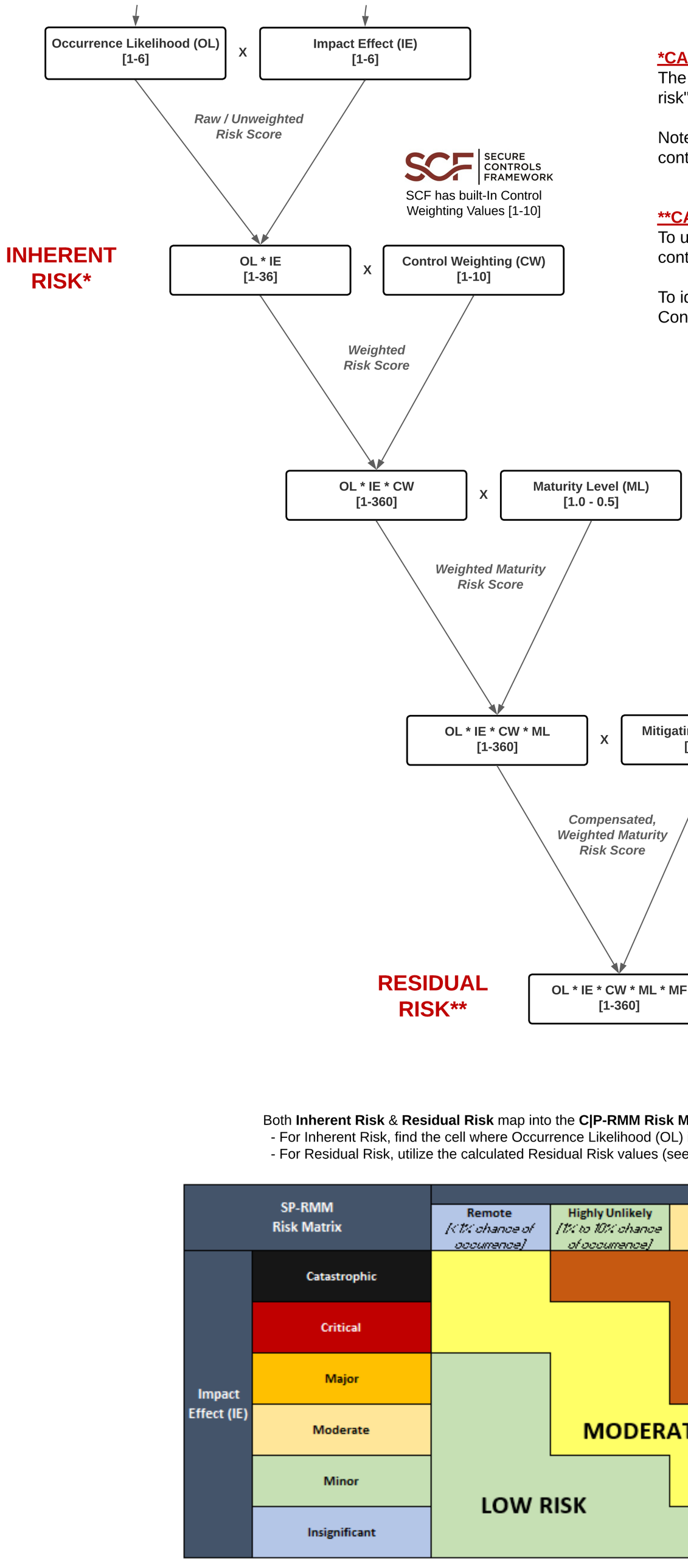
- **C|P-CMM 0 Not Performed** — Non-Existent Practices
- **C|P-CMM 1 Performed Informally** — Ad Hoc Practices
- **C|P-CMM 2 Planned & Tracked** — Requirement-Driven Practices
- **C|P-CMM 3 Well Defined** — Enterprise-Wide Standardization
- **C|P-CMM 4 Quantitatively Controlled** — Metrics-Driven Governance
- **C|P-CMM 5 Continuously Improving** — World-Class Practices

Calculating Risk Using The Cybersecurity & Data Privacy Risk Management Model (C|P-RMM)

version 2024.1

Occurrence Likelihood (OL)	Score	Description
Almost Certain	6	Virtual certainty the event will occur at some time, under normal business conditions, that can be quantified as greater than a 99% chance of occurrence.
Likely	5	Likely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 70%-99% chance of occurrence.
Possible	4	Reasonable to expect the event could occur at some time, under normal business conditions, that can be quantified as between a 25%-70% chance of occurrence.
Unlikely	3	Unlikely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 10%-25% chance of occurrence.
Highly Unlikely	2	Highly-unlikely event that can be quantified as between a 1%-10% chance of occurrence.
Remote	1	Theoretically possible. The likelihood of occurring can be quantified as less than a 1% chance of occurrence.

Impact Effect (IE)	Score	Description
Catastrophic	6	Critical, long-term damage or service impact. Financial and reputational damage could be enough to ruin the business.
Critical	5	Critical, short-term damage or service impact. Financial and reputational damage could create noticeable loss of market share.
Major	4	Major damage or service impact. Extensive reputational and financial impact, but not enough to ruin the business.
Moderate	3	Noticeable damage or service impact. Harmful reputational and financial impact, but not enough to ruin the business.
Minor	2	Localized or minimal damage or service impact. Minor reputational and financial impact.
Insignificant	1	Little to no damage or service impact. No reputational or financial impact.



CALCULATING INHERENT RISK: *[OL * IE]

The Occurrence Likelihood (OL), in combination with the Impact Effect (IE) will provide the "inherent risk" score.

Note - Inherent risk does not take into account any control weighting, the maturity of implemented controls or any other mitigating factors.

****CALCULATING RESIDUAL RISK: *[OL* IE * CW * ML * MF]***

To understand the "residual risk" that takes into account control weighting, the maturity of implemented controls and other mitigating factor, it requires expanding upon inherent risk calculations.

To identify the residual risk score, Occurrence Likelihood (OL) is calculated by Risk Impact Effect (IE), Control Weighting (CW), Maturity Level (ML) and Mitigating Factors (MF).

Maturity Level (ML)	ML Description	ML Value
0	Not Performed	1.0
1	Performed Informally	1.0
2	Planned & Tracked	0.9
3	Well Defined	0.7
4	Quantitatively Controlled	0.6
5	Continuously Improving	0.5

Mitigating Factor (MF)	Risk Reduction	MF Value
N/A - Not Required	Not Applicable	1.0
No Mitigating Factors Available	0%	1.0
Minimal Impact Reduction (Occurrence and/or Impact)	10%	0.9
Moderate Impact Reduction (Occurrence and/or Impact)	30%	0.7
Significant Impact Reduction (Occurrence and/or Impact)	50%	0.5

Risk Level	Residual Risk Values
Low	0.25 <= 36
Moderate	>36 <= 108
High	>108 <= 198
Severe	>198 <= 288
Extreme	>288 <= 360

Both **Inherent Risk** & **Residual Risk** map into the **C|P-RMM Risk Matrix** (graphic shown below.

- For Inherent Risk, find the cell where Occurrence Likelihood (OL) intersects Impact Effect (IE) to determine the risk level.
- For Residual Risk, utilize the calculated Residual Risk values (see chart above) to determine the corresponding risk level.

COMPLIANCE FORGE
www.ComplianceForge.com

SECURE CONTROLS FRAMEWORK
www.SecureControlsFramework.com