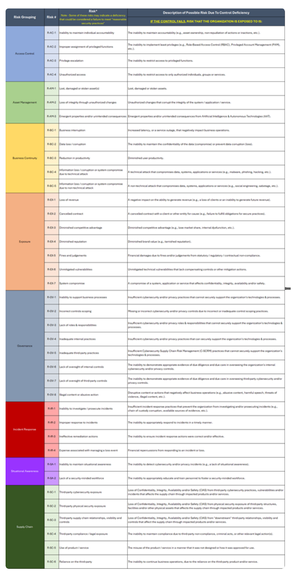
Cybersecurity & Data Privacy Risk Management Model (C|P-RMM)

version 2024.2



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.

** 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)

Category	System cybersecurity & data protection 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

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.

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.

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.

***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).

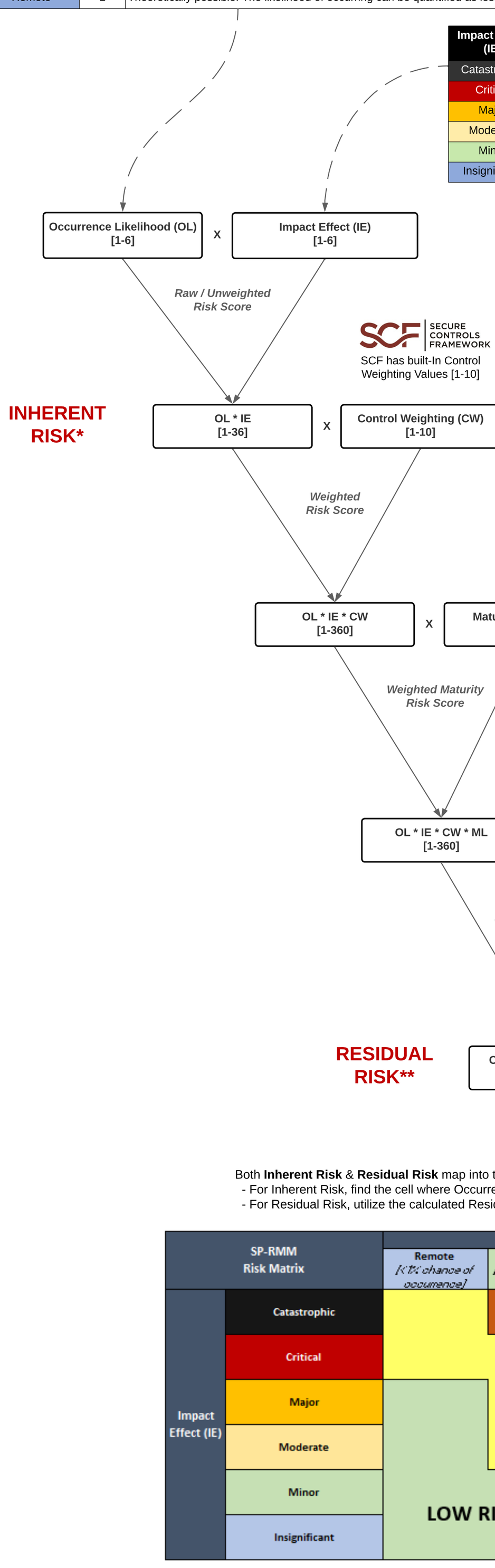
[continuous risk monitoring & assessments]

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

version 2024.2

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).

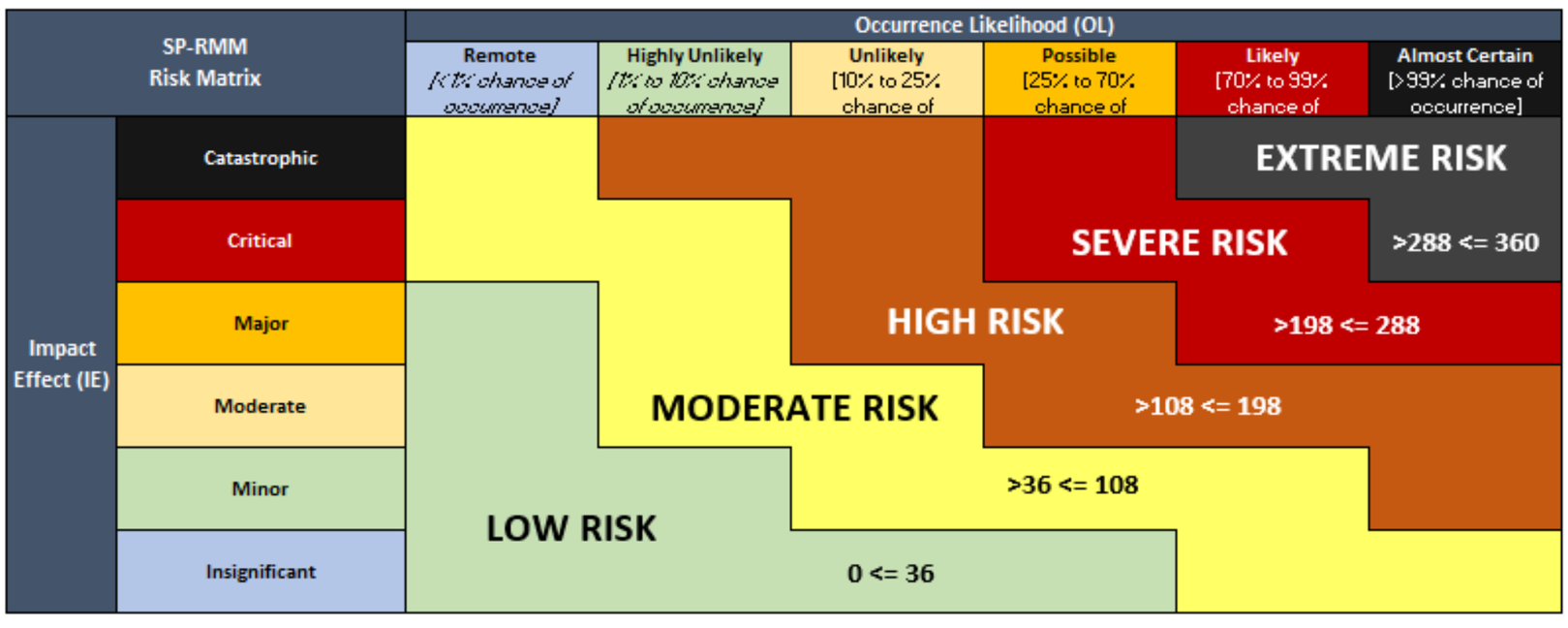
Maturity Level (ML)	ML Description	ML Value
0	Not Performed	1.0
1	Performed Informally	1.0
2	Planned & Tracked	0.9
3	Well Defined	0.7
4	Quantitatively Controlled	0.6
5	Continuously Improving	0.5

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.



www.ComplianceForge.com

www.SecureControlsFramework.com