

Security & Privacy Risk Management Model (SP-RMM)

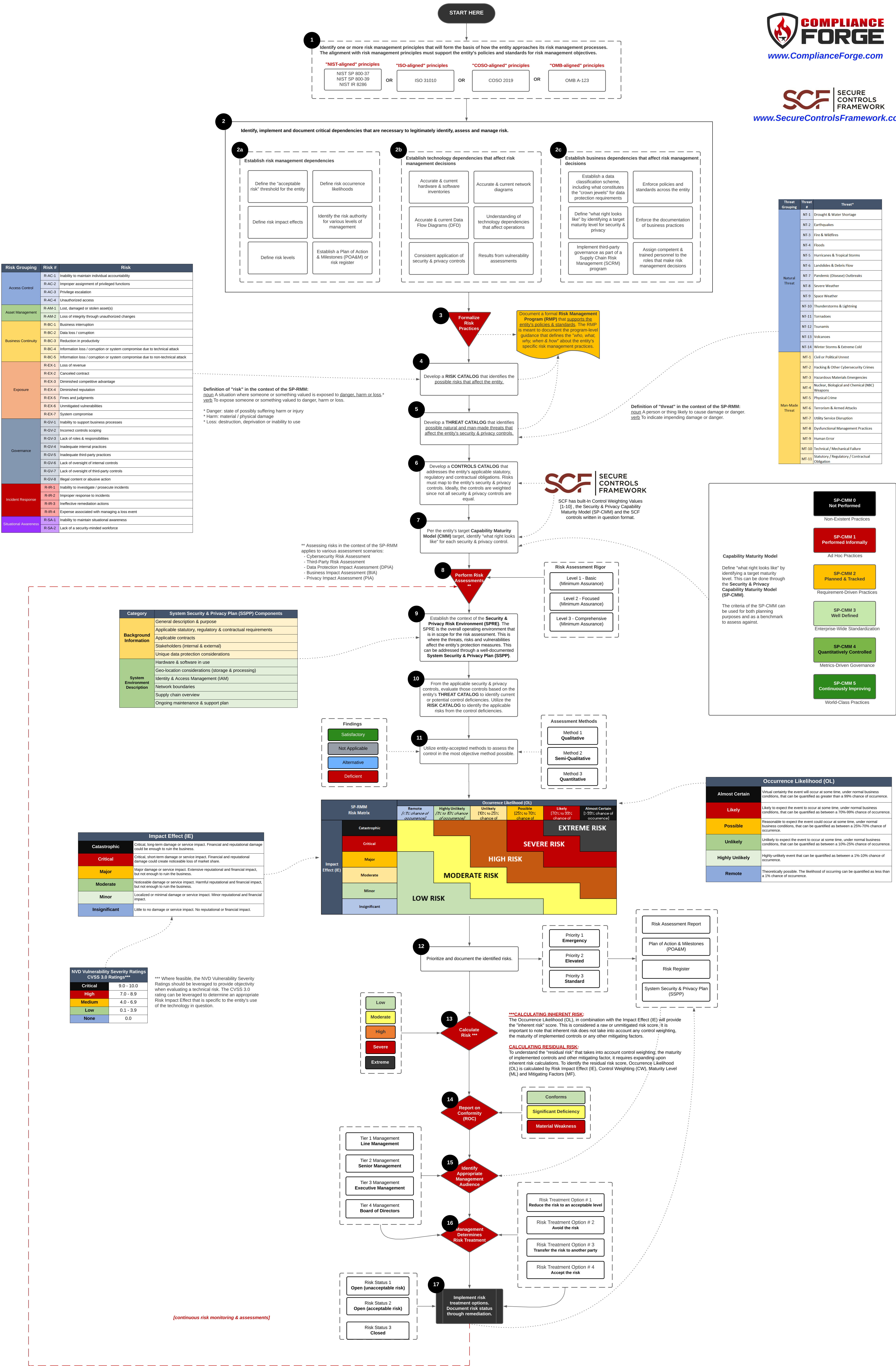
version 2022.2



www.ComplianceForge.com

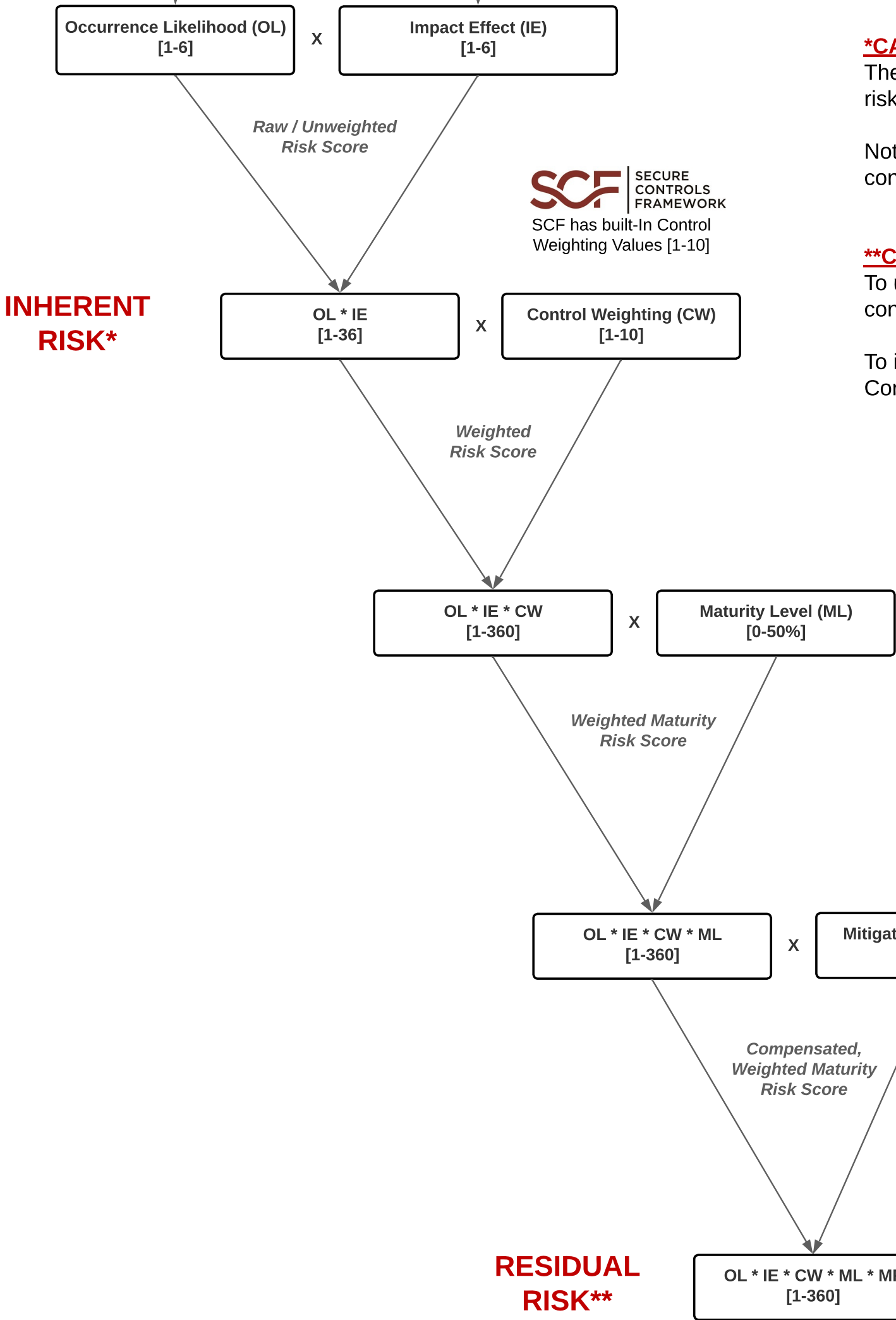


www.SecureControlsFramework.com



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	1 <= 36
Moderate	>36 <= 108
High	>108 <= 198
Severe	>198 <= 288
Extreme	>288 <= 360

Both **Inherent Risk** & **Residual Risk** map into the **SP-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.

