525 Wythe Street Alexandria, VA 22314 ▪ Phone: 703.299.9171 ▪ Fax: 703.995.4927

How TrustedAgent Manage Risk Assessment?

Risk management can be facilitated qualitatively and quantitatively at system, program, and organization level. Qualitative assessment is performed accordance to the guidance provided by NIST 800-30 Revision 1, and risk value is subsequently defined as Low, Moderate or High.

Quantitative analysis is also possible using TrusteAgent method below, and is based on each control. Once quantified, the derived values are mapped back to a qualitative measure previously discussed. This technique allows risk level to be quantified the same way and be compared across security controls for a particular system, group of systems under a particular program, and under an organization.

Risk Level for a given system can be measured as the products of:

RISK LEVEL = Vulnerability Level x Threat Level x Significance Level

Determination of Vulnerability Level

Vulnerability Level is a measurement of having a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability Level

Exploitability:	3
Objective Countermeasure:	2
Actual Countermeasure:	2.0
Vulnerability Score:	1
Vulnerability Level:	LOW

Vulnerability Level = Exploitability - Actual Counter Measures

Vulnerability Level	Vulnerability Score (Min)	Vulnerability Score (Max)
Low	1	2
Moderate	3	3
High	4	5

Exploitability (EXP): All systems are exploitable to certain extent in a presence of one or more threats through threat agents. The *theoretical* exploitability varies from 5=highly vulnerable to 1=low vulnerable. Note that there is no 'not vulnerable' value as a threat may not be known until it is exploited. Case in point, zero days attacks are examples of threats that are not known, thus are not defensible on the initial onset.

Objective Countermeasure (OCM): This is a ***practical*** value that represents the exploitability of the particular control. The term practical is utilized as no single system can be fully secured (i.e. 'risk-free'), and therefore, OCM is automatically defined as the EXP -1 to imply that there is ALWAYS some level of residual risk.

Actual Counter Measure (ACM): This is a calculated value of the exploitability of the control, and is dependent on the successful completion of the number of test cases. For each successful test case completion, the ACM would be increased by the value of OCM divides by the number of test cases. For example, if a control has five (5) test cases, with an OCM of 4, and all five are completed, the ACM would be 4. If four test cases were completed, the value for ACM would be 3.2. If one test case was completed, the ACM value would be 0.8.

The Vulnerability Level is then computed as EXP - ACM and be interpreted to a Vulnerability Level as indicated depending on its value.

Determination of Threat Level

Threat level measures any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat Level

Capability:	0
History:	0
Gain:	2
Attributability:	2
Detectability:	1
Threat Score:	1
Threat Level:	LOW

Threat Level = Capability + History + Gain - Attributability - Detectability

Threat Level	Threat Score (Min)	Threat Score (Max)
Low	1	2
Moderate	3	4
High	5	6

Capability (CAP): This is a measurement of the capability a threat can exert against a control or an asset. This is measured as an integer from 0 = None, or 1=Low to 3=High.

History (HIS): This is an indication of whether or not this threat has been exerted previously. If so, there likelihood of repeat attack will be there. This is measured as an integer from 0 = None, or 1=Low to 3=High.

Gain (GAIN): This is a measurement if a threat/attack was able to gain access to the asset or the control. This is measured as an integer from 0 = None, or 1=Low to 3=High.

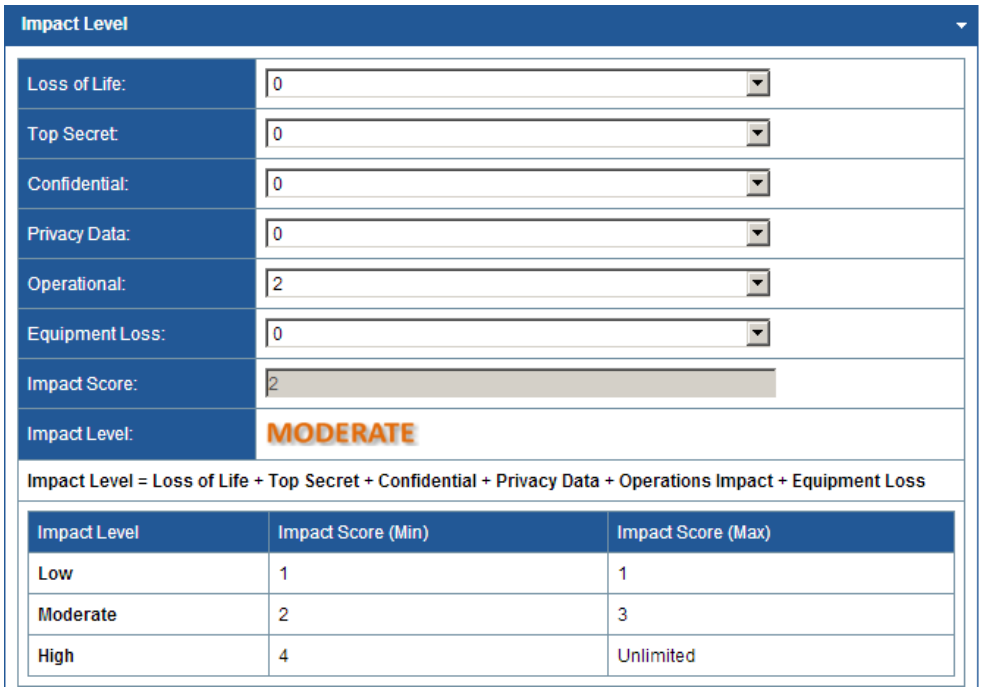
Attributability (ATTRIB): This value represents the complexity of the threat to be implemented. This is measured as an integer from 0 = Not complex, or 1=Low complexity to 3=High complexity.

Detectability (DETECT): This value represents whether the threat can be detected. This is measured as an integer from 0 = Cannot be detected, or 1=Low detection to 3=High detection.

The Threat Level is computed as CAP + HIS + GAIN – ATTRIB - DETECT, and the result is interpreted as shown.

Determination of Impact Level

Impact level measures the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.



Impact Level	Impact Score (Min)	Impact Score (Max)
Low	1	1
Moderate	2	3
High	4	Unlimited

Loss of Life: This is a measurement of the likelihood of loss of life. This is measured as an integer from 0 = None, or 1=Low to 3=High.

Top Secret: This is a measurement of the likelihood of loss of highly top secret or highly sensitive data. This is measured as an integer from 0 = None, or 1=Low to 3=High.

Confidential: This is a measurement of the likelihood of loss of confidential. This is measured as an integer from 0 = None, or 1=Low to 3=High.

Privacy Data: This is a measurement of the likelihood of loss of privacy data. This is measured as an integer from 0 = None, or 1=Low to 3=High.

Operational: This is a measurement of the likelihood of impact to the overall operation. This is measured as an integer from 0 = None, or 1=Low to 3=High.

Equipment Loss: This is a measurement of the likelihood of impact to the equipment sustaining the operation. This is measured as an integer from 0 = None, or 1=Low to 3=High.

The Impact Level is computed as Loss of Life + Top Secret + Confidential + Privacy Data + Operational + Equipment Loss, and the result is mapped to the level as shown.

Determination of Risk Level for the Control

The risk level represents the known risk based on the control implementation and assessment outcomes. This risk level is considered to be 'UNTREATED' as identified findings may have not been remediated through a plan of corrective actions.

In TrustedAgent's risk model, risk level is a measure of the extent to which an entity is threatened by having weakness(es), a potential circumstance or event, and typically a function of:

(i) Vulnerability Level
(ii) Threat Level
(iii) Impact Level

Control Risk

*Control:	CMR-6
Risk Score:	2
Risk Level:	LOW

Risk Level = Vulnerability Level x Threat Level x Impact Level

Risk Level	Risk Score (Min)	Risk Score (Max)
Low	0	18
Moderate	19	54
High	55	Unlimited

The product of the Vulnerability Level, Threat Level, and Impact Level represents the Risk Level of a system. This value is unbounded and distributed into qualitative scale as indicated above.

It is important to understand that the risk level calculated is based on that specific control using the risk score parameters defined for the control, and that the risk is untreated based on the implementation and assessment outcomes of the control. By refining the parameters associated with the control, one can emphasize the importance or significance of one control over another, more or less as appropriate. Untreated risks should be managed through corrective actions allowing the untreated risks to be reduced through remediation. The combination of the risk values and risk treatment and remediation is highly valuable in defining and maintaining consistent risk standards for an organization as part an overall enterprise risk management framework.

Determination of Total Risk of a System or Program or Site

Total risks of an entity (system, program or site) can be represented by the sum of the individual risk level for each of the applicable controls.

TOTAL UNTREATED RISK = $(\frac{1}{n}) \sum_{k=1}^{n} (\text{Risk Level})_k$, where n= the number of applicable controls, and k=first control

The Total Untreated Risk should map back to the Risk Level as defined below.

Risk Level	Risk Score (Min)	Risk Score (Max)
Low	0	18
Moderate	19	54
High	55	Unlimited

As risks are remediated through implemented corrective actions, the total untreated risks should be decreasing (i.e. improving) to indicate improved implementation and effectiveness of the implemented controls. Total untreated risks provides excellent indication of the risk posture for an assessment entity, in real-time and from historically perspective.

Corrective actions also provide another important measurement to the risk management process. As more corrective actions are required to address the identified weaknesses or findings, the sum of the total risks associated with the corrective actions must increase. This sum represents the total risks would be offset against the total untreated risks if the corrective actions are fully implemented and effective. The sum provides indication into the amount of resources to be assigned for remediation.

The difference between the sum of the treated risks and the untreated risks is the residual risk of the entity, and the key value in determining risk acceptance for a system or program under an authorization program.

the risk levels contributed to the total risk from the impact controls would be reduced and one would subsequently expect a reduction to the TOTAL RISK score from historical (pre-treated risks). Corrective actions, even though, may contain risk levels, they represent the outstanding risks being