CYBERSECURITY RISK MANAGEMENT POLICY

Purpose

To empower the security team to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope

Risk assessments can be conducted on any entity within CINDAS LLC or any outside entity that has signed a *License Agreement* with CINDAS LLC. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy

The execution, development, and implementation of remediation programs is the joint responsibility of CINDAS LLC and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the CINDAS LLC Risk Assessment Team in the development of a remediation plan.

For additional information, go to the ***Risk Assessment Process*****.**

Policy Compliance

Compliance Measurement
The RA team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal, and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the RA team in advance.

Non-Compliance
Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of access.

Risk Assessment Process

Step 1: Determine the scope of the risk assessment

Decide what is in the scope of the assessment. Is it the entire organization, or a business unit, location or a specific aspect of the business, such as payment processing or a web application? Have the full support of all stakeholders whose activities are within the scope of the assessment as their input will be essential to understanding which assets and processes are the most important, identifying risks, assessing impacts, and defining risk tolerance levels. A third-party specializing in risk assessments may be needed to help them through what is a resource-intensive exercise.

Step 2: Identify cybersecurity risks

2.1 Identify assets

The next task is to identify and create an inventory of all physical and logical assets that are within the scope of the risk assessment. When identifying assets, it is important to not only establish those which are considered the CINDAS LLC's assets critical to the business and probably the main target of attackers, but also assets attackers would want to take control over, such as a server or archives and communications systems, to use as a pivot point to expand an attack. Create a network architecture diagram from the asset inventory list to visualize the interconnectivity and communication paths between assets and processes as well as entry points into the network, making the next task of identifying threats easier.

2.2 Identify threats

Threats are the tactics, techniques, and methods used by threat actors that have the potential to cause harm to an organization's assets. To help identify potential threats to each asset use a threat library and security vendor reports and advisories from government agencies.

2.3 Identify what could go wrong

This task involves specifying the consequences of an identified threat exploiting a vulnerability to attack an in-scope asset. For example:

Threat: **An attacker performs an SQL injection on an**

Vulnerability: **unpatched**

Asset: **web server**

Consequence: **customers' private data stolen, resulting in regulatory fines and damage to reputation.**

Summarizing this information in simple scenarios like this makes it easier for all stakeholders to understand the risks they face in relation to key business objectives and for security teams to identify appropriate measures and best practices to address the risk.

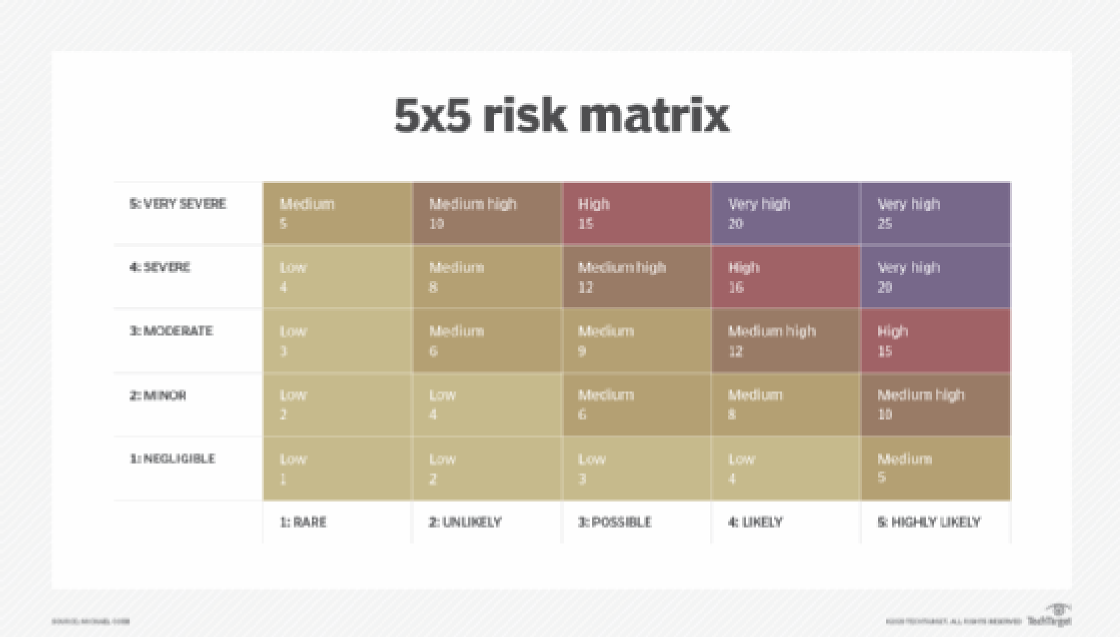
Step 3: Analyze risks and determine potential impact

Risk likelihood -- the probability that a given threat is capable of exploiting a given vulnerability -- should be determined based on the discoverability, exploitability, and reproducibility of threats and vulnerabilities rather than historical occurrences. Ranking *likelihood* on a scale of 1: Rare to 5: "Highly Likely," and *impact* on a scale of 1: Negligible to 5: "Very Severe," makes it straightforward to create the risk matrix illustrated below in Step 4.

Impact refers to the magnitude of harm to the organization resulting from the consequences of a threat exploiting a vulnerability. The impact on confidentiality, integrity and availability should be assessed in each scenario with the highest impact used as the final score. This aspect of the assessment is subjective in nature, which is why input from stakeholders and security experts is so important.

Step 4: Determine and prioritize risks

Using a risk matrix like the one below where the risk level is "Likelihood times Impact," each risk scenario can be classified.



5x5 risk matrix

5: VERY SEVERE	Medium 5	Medium high 10	High 15	Very high 20	Very high 25
4: SEVERE	Low 4	Medium 8	Medium high 12	High 16	Very high 20
3: MODERATE	Low 3	Medium 6	Medium 9	Medium high 12	High 15
2: MINOR	Low 2	Low 4	Medium 6	Medium 8	Medium high 10
1: NEGLIGIBLE	Low 1	Low 2	Low 3	Low 4	Medium 5
	1: RARE	2: UNLIKELY	3: POSSIBLE	4: LIKELY	5: HIGHLY LIKELY

TechTarget

Any scenario that is above the agreed-upon tolerance level should be prioritized for treatment to bring it within the organization's risk tolerance level. There are three ways of doing this:

1. **Avoid.** If the risk outweighs the benefits, discontinuing an activity may be the best course of action if it means no longer being exposed to it.
2. **Transfer.** Share a portion of the risk with other parties through outsourcing certain operations to third parties such as DDoS mitigation, or purchasing cyber insurance. First-party coverage generally only covers the costs incurred due to a cyber event such as informing customers about a data breach, while third-party coverage would cover the cost of funding a settlement after a data breach along with penalties and fines. What it will not cover are the intangible costs of loss of intellectual property or damage to brand reputation.

3. **Mitigate.** Deploy security controls and other measures to reduce the Likelihood and/or Impact and therefore the risk level to within the agreed risk tolerance level. Responsibility for implementing the measures to reduce unacceptably high risks should be assigned to the appropriate team. Dates for progress and completion reports should also be set to ensure that the owner of the risk and the treatment plan are kept up to date.

However, no system or environment can be made 100% secure, so there is always some risk left over. This is called residual risk and must be formally accepted by senior stakeholders as part of the organization's cybersecurity strategy.

Step 5: Document all risks

It's important to document all identified risk scenarios in a risk register. This should be regularly reviewed and updated to ensure that management always has an up-to-date account of its cybersecurity risks. It should include:

- Risk scenario
- Identification date
- Existing security controls
- Current risk level
- Treatment plan -- the planned activities and timeline to bring the risk within an acceptable risk tolerance level along with the commercial justification for the investment
- Progress status -- the status of implementing the treatment plan
- Residual risk -- the risk level after the treatment plan is implemented
- Risk owner -- the individual or group responsible for ensuring that the residual risks remain within the tolerance level

A cybersecurity risk assessment is a large and ongoing undertaking, so time and resources need to be made available if it is going to improve the future security of the organization. It will need to be repeated as new cyber threats arise, and new systems or activities are introduced, but done well first time around it will provide a repeatable process and template for future assessments, whilst reducing the chances of a cyber-attack adversely affecting business objectives.

Sources:

Risk Assessment Policy: https://eriskeplhelpline.enquiron.com/App/Resources

Risk Assessment Process: https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step