Risk Assessment Procedures

MK Agents

Risk assessments are key in IT security, as they allow for the identification and management of potential risks to security and information. Preventing and managing risks helps save money, trust, and time. Below is a set of risk assessment procedures that should be followed to protect MK Agents' digital security.

Key Steps

The key steps to risk assessments are;

- *Risk identification*
- *Measure the impacts of the risk*
- *Record risk management*
- *Take action to reduce risk*
- *Review the application of the risk assessment*

(Worksmart, 2019) (Burgon, 2013) (HSE UK, n.d.)

Risk Identification

Using this information, it's possible to outline a step by step process for executing a risk management for IT Infrastructure. The first step, risk identification, involves using various techniques to identify risks within the infrastructure, including a penetration-test, an ST&E, or a tool that scans the network for vulnerabilities (Sotnikov, 2018). These all help expose issues that a network may have and helps implement solutions by identifying the root causes.

Security Test and Evaluations are often conducted alongside Security Control Assessments (HHS Cybersecurity Program, n.d.), and focus on evaluating the requirements for safeguards for information and the overall safety of a system (Cybrary, 2018). An SCA alongside this helps check the efficacy of applied security controls, such as firewall rules and access restriction (Pfleeger & Pfleeger, 2003). These together help identify some key areas of risk for systems and infrastructure.

A penetration test (or pen-test) involves simulating a cyberattack, with the goal to be to be the identification of cybersecurity risks like vulnerable systems, topologies or software. These can be key to the identification of risks and vulnerabilities, as a simple vulnerability assessment is less in-depth and may miss key issues that would only be identifiable by a hacker or pen-tester. (Cisco, n.d.)

Vulnerability Scanning Tools help automate the procedure of identifying risks, with tools that scan with a range from the source code of implemented software, all the way up to system or network scanners (Gregg, 2007). These tools are significant as they can spot issues that a pen-tester or an ST&E or STA might miss, as they're automated and don't have the possibility of human error.

Measuring the impact of the risk

The next step following the identification of risks involves analysing the impact they'd have on network security, company operations, individual health and user safety. Usually this can be easily identified, however having a catalogue of computer hardware, network topology diagrams, and a description of data storage can help identify which risks are more significant and the extent they might have. For example, a threat that exposes user data remotely may be more significant than a threat that requires direct access to the company ethernet (Sotnikov, 2018).

The frequency or probability at which a risk may arise is also important to take into consideration, as an issue that is statistically unlikely to occur may be less significant than a misconfigured firewall, for example. Working out how often or how likely it is that a risk arises relies on understanding of the root cause.

Documents such as a Business Impact Analysis may also assist with the measurement of the impact of a risk (Sotnikov, 2018), which help to measure the impact of risks using a short description of each and how much it is likely to cost the business (Ready.gov, n.d.). There are worksheets that can be filled out and utilised for this purpose, usually including a table like so;

Timing/Duration	Operational Impacts	Financial Impacts

(FEMA, n.d.)

This sheet helps describe the differences between risks, focussing on the duration of interruption or financial impacts, the operational impacts such as lost sales or regulatory fines, and the predicted quantity of the financial impact that each issue may result in (FEMA, n.d.).

Record Risk Management & Review of Application

Risk assessments rely upon a standard model of risk assessment sheets, that outline the risk itself, the severity and likelihood, the proposed solution, then another analysis of the risk following the solution being applied. An example of a risk assessment sheet demonstrating a potential risk and a solution is as follows:

Risk Description	Severity	Likelihood	Solution	Continued Severity	Continued Likelihood
Power outages	7/10	Rare	Purchase an Uninterrupted Power Supply (UPS) for essential systems.	1/10	Rare

(Smartsheet, 2019)

This example sheet outlines a simple layout for a risk management sheet, which can be extended to fit more complex issues and severity descriptions, as well as prescribing who should solve the risk and when it should be done by. It also includes a section that evaluates the effectiveness of the solution, which again can be extended to be more comprehensive. This section allows for an iterative risk management approach, where risks are only considered solved after they reach an 'allowed' threshold of severity.

Explanation of ISO 31000

ISO 31000 is a set of risk management guidelines, principles, frameworks and processes designed to help manage risks (ISO, 2018). It is produced and distributed by the International Organisation for Standardisation, or ISO (ISO, n.d.). This standard helps to implement some standard features of risk management with detailed explanations of implementation and utilisation, useable in most cases where a business or organisation faces risk (ISO, 2018).

ISO 31000 is applicable as a framework for MK Agents, as it outlines security frameworks in better detail than outlined in this document, and the content can be customised to better suit the application required. ISO 31000 also outlines 11 key principles for risk management, applicable at the discretion of the business.

> 1. *Risk management establishes and sustains value.*
> 2. *Risk management is an integral part of all organizational processes.*
> 3. *Risk management is part of decision making.*
> 4. *Risk management explicitly addresses uncertainty.*
> 5. *Risk management is systematic, structured, and timely.*
> 6. *Risk management is based on the best available information.*
> 7. *Risk management is tailored.*
> 8. *Risk management takes human and cultural factors into account.*
> 9. *Risk management is transparent and inclusive.*
> 10. *Risk management is dynamic, iterative, and responsive to change.*
> 11. *Risk management facilitates continual improvement of the organization.*

(Hutchins, 2019)

Using these principles makes the process of applying risk management practises and procedures safer and easier, being comprehensive in the application and requirements that a risk management structure should have.

References

Burgon, R., 2013. *The Five Step Guide to Risk Assessment.* [Online]
Available at: https://rospaworkplacesafety.com/2013/01/21/what-is-a-risk-assessment/
[Accessed 4th December 2019].

Cisco, n.d.. *What Is Penetration Testing?.* [Online]
Available at: https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html
[Accessed 4th December 2019].

Cybrary, 2018. *What is Security Test & Evaluation (ST&E)?.* [Online]
Available at: https://www.cybrary.it/glossary/s-the-glossary/security-test-evaluation-ste/
[Accessed 4th December 2019].

FEMA, n.d.. *Business Impact Analysis Worksheet.* [Online]
Available at: https://www.fema.gov/media-library-data/1388776348838-b548b013b1cfc61fa92fc4332b615e05/Business_ImpactAnalysis_Worksheet_2014.pdf
[Accessed 4th December 2019].

Gregg, M., 2007. *Automated Assessment Tools.* [Online]
Available at: https://flylib.com/books/en/1.36.1/automated_assessment_tools.html
[Accessed 4th December 2019].

HHS Cybersecurity Program, n.d.. *Security Control Assessment & Security Test and Evaluation.* [Online]
Available at: https://irtsectraining.nih.gov/ISITAdmin_2017/rolebasedtraining-itadmin/part39.htm
[Accessed 4th December 2019].

HSE UK, n.d.. *Managing risks and risk assessment at work.* [Online]
Available at: https://www.hse.gov.uk/simple-health-safety/risk/steps-needed-to-manage-risk.htm
[Accessed 4th December 2019].

Hutchins, G., 2019. *ISO 31000 Principles of Risk Management.* [Online]
Available at: https://accendoreliability.com/iso-31000-principles-risk-management/
[Accessed 17th December 2019].

ISO, 2018. *ISO 31000 Risk management.* [Online]
Available at: https://www.iso.org/iso-31000-risk-management.html
[Accessed 9th December 2019].

ISO, 2018. *ISO 31000:2018(en).* [Online]
Available at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en
[Accessed 9th December 2019].

ISO, n.d.. *ISO name and logo.* [Online]
Available at: https://www.iso.org/iso-name-and-logo.html
[Accessed 9th December 2019].

Pfleeger, S. L. & Pfleeger, C. P., 2003. *Security in Networks.* [Online]
Available at: http://www.informit.com/articles/article.aspx?p=31339&seqNum=3
[Accessed 4th December 2019].

Ready.gov, n.d.. *Business Impact Analysis.* [Online]
Available at: https://www.ready.gov/business-impact-analysis
[Accessed 4th December 2019].

Smartsheet, 2019. *All the Risk Assessment Matrix Templates You Need.* [Online]
Available at: https://www.smartsheet.com/all-risk-assessment-matrix-templates-you-need
[Accessed 4th December 2019].

Smartsheet, 2019. *Risk Management Matrix (Example).* [Online]
Available at: https://www.smartsheet.com/sites/default/files/2019-11/IC-Risk-Management-Matrix-8849_PDF.pdf
[Accessed 4th December 2019].

Sotnikov, I., 2018. *How to Perform IT Risk Assessment.* [Online]
Available at: https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/
[Accessed 4th December 2019].

Worksmart, 2019. *What are the five steps to risk assessment?.* [Online]
Available at: https://worksmart.org.uk/health-advice/health-and-safety/hazards-and-risks/what-are-five-steps-risk-assessment
[Accessed 4th December 2019].