5 Risk assessment

This chapter of the Toolkit is devoted to the subject of information security risk assessment and management. Information risk management is important as organisations cannot avoid being exposed to information risk. It forms part of Stage 2 – Planning, assessment and evaluation, Stage 3 – Implementation, support and operation and Stage 4 – Performance, evaluation and improvement in the Toolkit Route map.

Within this chapter, a methodology for information risk assessment is described, as well as some of the key considerations involved when carrying out information security risk assessment.

It is important to ensure that any corporate risk management strategy, risk management method and assessment methods are borne in mind when carrying out information security risk assessments.

Key topics

- **Why information security risk assessment is important**
- **The key steps in carrying out an information security risk assessment**
- **How to decide the appropriate cost of mitigating an information risk**

Carrying out and documenting information risk assessments provides for an auditable process, demonstrating and providing justification for decisions made in relation to information security.

Organisations wishing to achieve certification to ISO/IEC 27001 should note that (as per clauses 8.2 and 8.2 of ISO/IEC 27001) they should carry out information security risk assessments, keep records of those information risk assessments and use the information risk treatment plan derived from the information risk assessments to treat the documented information risks.

The exact risk assessment methodology to be used is not specified by the Standard. Organisations can choose to follow the approach described here, or another approach which suits them better.

5.1 Information risk management

Information risk management is the systematic identification and assessment of information risk, coupled with the consideration, planning and application of risk responses, in order to ensure that the exposure to a given risk is at an acceptable level. It is an iterative process which, due to the ever changing internal and external environments and the emergence of new threats and identification of new vulnerabilities, is never complete.

All organisations have information assets. These information assets are often critical in supporting business operations. Equally, all organisations are exposed to threats and vulnerabilities which constitute risks to those information assets and if left unchecked have the potential to damage the organisation's ability to meet its stated objectives.

As such it is prudent to consider the risks which may have a negative impact on their information assets and, through the consistent application of information risk assessments, determine the controls they wish to apply to treat the risks to those assets.

The extent to which an organisation invests resource in protecting its information assets should be directly related to the potential impact of the risks on those assets.

Only by carrying out information security risk assessments to identify and assess all the risks facing its information assets can an organisation hope to identify how to best utilise its resources to treat those risks. Additionally carrying out and documenting information risk assessments provides for an auditable process demonstrating and providing justification for decisions made in relation to information security.

Each organisation should determine the specific threats which affect the confidentiality, integrity and availability of their information assets.

Whilst this toolkit is written from the perspective of risk assessing information assets, it is important to note this is not the only approach. For those pursuing certification against ISO/IEC 27001:2013, the latest version of the standard does not require an information asset-based approach. However, certainly in the short term this is what auditors will be used to seeing, and it will not invalidate an ISMS from their perspective. Regardless of the risk assessment methodology chosen, the essential steps of information risk identification followed by assessment of impact and likelihood still apply.

The reading list for this chapter contains links to examples of established best practice.

5.2 Define information risk measurement criteria

Whilst information security risk assessment is a distinct activity, it is important to ensure that any corporate information risk management strategy, information risk management method and assessment methods are borne in mind when carrying out information security risk assessments. This is in order that the assessment of, and products from, information security risk assessments make sense in the context of the wider organisational risk management framework and fit into wider organisational and strategic risk registers.

It is also important to note that information risks can be mapped to the type of organisational objective concerned, that is to say strategic (long-term), programme/project (medium-term) and operational (short-term) objectives. The type of objective which an information risk affects will have some bearing on the level of audience who should be reviewing and managing the risk. However there may be interplay between the different levels. For example a project risk could quite easily be relevant in terms of the programme to which it belongs and potentially could affect a strategic objective. As such, risks identified at one level will often feature on the risk register at another.

Information risk assessments should consider impact in terms of the effect on the organisation's stated purpose and objectives.

The OCTAVE Allegro guidebook V1.0 on information security risk assessment suggests that as a minimum the following impact areas are considered: reputation/customer confidence, financial, productivity, safety and health, fines/legal penalties, plus one or more user-defined impact areas.

5.3 Information asset identification and profiling

An information asset is essentially a distinct set of information which has some value to the organisation. Every organisation will have thousands, or even millions, of information assets, and it is infeasible to expect to identify and profile each one individually. However, many assets will be sufficiently similar that they can be addressed in aggregate, while a few (e.g. certain research data sets) will be unique and valuable/critical enough to warrant individual attention.

When evaluating risk against an information asset, it is important to have a sufficient understanding of the information asset (or class of assets).

The organisation should develop a profile which covers:

- exactly what the asset is
- its requirements for confidentiality, integrity and availability
- the lifecycle of the asset (some assets, such as research findings, experience a change in their requirements for confidentiality after publication)
- the business processes which affect it
- ownership
- the value of the asset to the organisation, and why the asset is important to the organisation
- the expected value of the asset to an attacker
- its classification (see Chapter 7, Information management)
- its expected lifespan.

It is also important to understand where the information asset is located in terms of information asset

"containers" i.e. the information asset may be more or less vulnerable to a specific threat depending on the systems or storage locations in which it is held through the information lifecycle. Information may be more vulnerable to disclosure during transmission as opposed to processing or storage.

A clear understanding of the asset enables better understanding of the threats and vulnerabilities and thus enables more effective information risk assessment.

5.4 Threat identification and assessment

Having identified and profiled the information asset, the next stage is to identify the threats to that information asset. This can be done by brainstorming or by reviewing a list of common threats and identifying which threats are relevant. Some typical threat categories include: natural disaster, human, competitors, criminals, political. However each organisation should determine the specific threats which affect the confidentiality, integrity and availability of their information assets. Threat identification can be carried out in a hierarchical fashion, starting with the business and strategic threats and then working down to technical threats and relating them to strategic and business threats.

When performing risk assessments, because of the subjective nature of this approach, it is recommended that risks are assessed by more than one person.

When carrying out a threat assessment, each identified threat should be classified and ranked according to potential impact. There are a range of models which can be used to rank threats. Typically they will include some or all of the following:

- the potential damage
- how repeatable the attack/event is
- how easy it is to carry out the threat e.g. what skills might be required
- how easy it would be for a malicious party to discover the vulnerability
- motivation.

5.5 Identify and assess vulnerabilities

A vulnerability is a weakness that exposes an organisation to information risk by providing an attack surface for a threat. For example, a hacker can be seen as a threat, and a vulnerability that the hacker may exploit could be a poorly patched web server. The information risk is a combination of the threat of the hacker and the opportunity provided by the availability of the web server vulnerable to attack. The information risk can then be calculated by assessing the likelihood of the hacker attacking the webserver and multiplying it by the impact on the organisation of the attack. As with threat assessment, the likelihood and impact relating to each vulnerability should be assessed. As with threats, there are different aspects such as motivation, repeatability and how easy it is to exploit the vulnerability.

An information asset may be more or less vulnerable to a specific threat, depending on the way in which it is handled and stored.

With regard to types of vulnerabilities, it is possible to find lists of typical vulnerabilities online. For example, the Common Vulnerabilities and Exposures database is a freely available dictionary of publicly known information security vulnerabilities and exposures. However, information security vulnerabilities come in human, physical and process form as well as software and hardware. Identification of vulnerabilities can also be treated hierarchically, as for threats (see previous subsection).

The potential impact of each vulnerability should then be assessed and quantified in order to allow the highest priority vulnerabilities to be addressed first.

5.6 Scoring information risk impact assessment

Having identified the threats and vulnerabilities, the resultant information risks must be quantified. Since no organisation has unlimited resources to employ in the mitigation of risk and since different mitigation actions are more or less effective than each other, it is essential to understand which risks need to be addressed first, and what mitigation actions offer the most protection, for the least investment in time and effort.

5.6.1 Quantitative vs. qualitative information risk assessment

Qualitative information risk assessment is the most commonly used approach to information security risk assessment and uses subjective estimates (e.g. high, medium, low) for likelihood and loss/consequence. When performing information risk assessments, it is recommended that information risks are assessed by more than one person to reduce the subjective element of this approach. A workshop format is often a useful way of bringing those individuals who are most familiar with the information asset and the associated threats and

vulnerabilities together to discuss and agree the likelihood and impact of each risk. Examples of this type of information risk assessment can be seen in the resources section for this chapter.

Quantitative information risk assessment, unlike qualitative information risk assessment, uses numerical values (normally monetary) rather than subjective values (high, medium, low) for risk assessment. Figures are derived for the Single Loss Expectancy (how much the occurrence of a given information risk costs) and Annual Rate of Occurrence (how often a risk will occur per year). From these it is possible to calculate the Annual Loss Expectancy (how much the organisation can expect to lose each year for a given risk).

By defining a monetary value for risks and having the historic data to determine the expected frequency, it is not only possible to prioritise information risks in order of the financial impact on the organisation, but in combination with an understanding of the costs of your controls and their effectiveness at mitigating risk, it is possible to make some statements about the Return On Security Investment.

Unfortunately, quantitative information risk assessment requires a significant amount of data about information risk impacts and probabilities, which may not be readily available and which are resource intensive to collect. Calculations can be complex and resource intensive and, as a result, professional risk management software is often required for effective analysis. In addition, technology changes so fast that historical data may not be a good source of information about current and future impacts and probabilities.

It is often the case, particularly with information security risk, that the impact of a risk cannot be defined solely as a numerical value or monetary sum. For example, the reputational impacts of a data breach cannot easily be measured by quantitative methods. Quantitative information risk assessment is a process which requires experience and competence to use and is not as straightforward to involve colleagues in as qualitative information risk assessment.

One possible approach is to use qualitative information risk management by default, and quantitative information risk assessment where it is felt that the benefits provided by the technique outweigh the costs.

5.7 Process

The information risk assessment case study provides a practical example of how information risk measurement criteria can be used to help achieve consensus when using qualitative information risk assessment.

Since qualitative information risk assessment is largely subjective, agreement may not be reached if a simple high, medium, low rating is used to rate impact and likelihood. Using information risk measurement criteria provides a consistent basis on which to assess the impact and likelihood of a risk and provides a descriptor for each impact level and likelihood rating so that individual perceptions of what is high or low are excluded and consensus is reached on which impact statement best described the perceived risk.

The steps involved are:

1. Considering the threats and vulnerabilities, generate information risk scenarios (e.g. through brainstorming). These scenarios should, in real world terms, outline something which could go wrong and the mechanism by which it could occur. You can also use a standard list of risk scenarios.
2. Assess and score each information risk for impact.
3. Assess and score each information risk for likelihood.
4. Plot impact and likelihood of each information risk on a risk acceptance matrix (examples of which appear in the case studies supporting this chapter).

When describing risks, it is good practice to break the description down into a statement clarifying the cause, event and effect.

It is important to retain some sense of proportion when attempting to estimate impacts and effects; the organisation should bear in mind that some of the most devastating impacts actually rely on a chain of specific circumstances, which reduces the likelihood of an event with that very high impact occurring.

5.8 Information risk treatment

Having plotted the identified information risks on the information risk acceptance matrix, decisions (based on the organisation's information risk appetite) can be made as to the responses to be taken for each information risk. Typical risk treatment options include:

- terminate (cease the activity giving rise to the risk)
- transfer[1] (typically by passing some aspect of the risk onto another body such as an insurance company)
- reduce or increase (through applying, modifying or removing controls)

- accept (accept the risk).

When treating an information risk by implementing a control, an estimation should be made as to the effect of that control on the overall risk score (also see Chapter 6, Controls, for an overview of controls). In doing this, the residual risk score (amount of risk remaining) can be calculated and a decision made as to whether the residual score is still too high and further mitigation is required.

It is essential to understand which risks need to be addressed first, and what mitigation actions offer the most protection for the least investment in time and effort.

The organisation should ensure that the effort and expense involved in treating an information risk does not significantly exceed the loss (whether measured in financial, reputational, legal, ethical, etc. terms) which would be suffered should the risk materialise.

It is essential that, as part of the process, information risk owners and action owners are assigned. The information risk owner is the person or body which has the authority and accountability for managing an information risk. The action owner is the individual responsible for carrying out the activities to control the information risk. It is possible that the information risk owner and action owner may be the same person.

At a higher level, whether part of the organisation's pre-existing risk management framework or a specific information security governance body, there should be a review body which on a regular basis scrutinises the management of information security risk. See Chapter 2, Information security governance.

5.9 Information risk register

Identified information risks should be added to an information risk register outlining all the information risks faced by the organisation, what controls are being applied, and the initial, current and residual information risk scores. In this way, it is possible to see at a glance how exposure to an information risk has changed over time. Information risk management is a cyclical process, and risks should be reassessed on a regular basis (the degree of regularity depending on the significance of the risk) but also as part of managing changes to the operating environment. Changes in the threat landscape may allow the relaxation of certain controls or, equally, require extra controls.

A further reason for maintaining an information risk register is to provide an auditable account of decisions made. This will allow the organisation to manage identified information risks as well as to determine the overall information risk exposure. The register will also act as an historical record of the assessed value of each information risk over time.

It should be noted that information security risk assessment cannot be carried out and managed in isolation. Risks identified as part of the information security process should be integrated into the appropriate organisational risk registers. For example, information security risks which have the potential to impact on organisation strategies should be referenced from the organisation's overall strategic risk register.

Summary

- Information risk management is a systematic, consistent, iterative process where risks are identified and assessed before being treated and monitored
- Information risk treatment options should not cost more to deploy and manage than the cost of the risk itself
- Information risk management should not be done in a vacuum, but as part of the overall organisational risk management process

[1]NB: Risk transference cannot entirely mitigate a risk, as reputational risk tends to remain with the organisation (e.g. TKMaxx's incident was due to activities of a third party, yet it was TKMaxx which experienced the reputational damage).

Resources

Template for information risk management principles

Development and use of risk assessment templates - UCL, case study

Project information risk assessment – Requirements and expectations - UCL

Service information risk assessment – Requirements and expectations - UCL

Project information risk assessment – Capability - UCL

Service information risk assessment – Capability - UCL

Risk treatment plan – UCL

Risk assessment methodology – Cardiff University

Information asset register tool – University of Oxford

Reading list

A complete set of resources necessary to perform an information security assessment based on the OCTAVE Allegro method
www.ucisa.ac.uk/ismt21

www.cert.org/resilience/products-services/octave/octave-allegro-method.cfm

European Union Agency for Network and Information Security (ENISA) Risk Management Hub
www.ucisa.ac.uk/ismt22

www.enisa.europa.eu/activities/risk-management

ISO 31000:2009 Risk Management Principles and Guidelines
www.ucisa.ac.uk/ismt23

www.iso.org/iso/home/standards/iso31000.htm

University of Oxford Risk Assessment of Information Assets
www.ucisa.ac.uk/ismt24

http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/risk-assessment

Risk management in higher education - A guide to good practice, prepared for HEFCE by PricewaterhouseCoopers
www.ucisa.ac.uk/ismt25

http://dera.ioe.ac.uk/5600/

Higher Education Funding Council for England (HEFCE) strategic risk register in which 11 key risk areas are identified
www.ucisa.ac.uk/ismt26

http://webarchive.nationalarchives.gov.uk/20100202100434/http://www.hefce.ac.uk/about/standards/howweareaccountable/riskman/