Unit 7 Risk Management

Site: Moodle - Edinburgh Napier University
Course: INF11109 2019-0 TR1 001 - Security Audit & Compliance
Workbook: Unit 7 Risk Management
Printed by: Timothy Muscat
Date: Monday, 4 November 2019, 1:22 PM

Table of contents

Introduction

This unit deals with risk management, building on the concepts of information asset, threat, vulnerability and attack that were introduced in Unit 1. You will learn about risk management concepts (including threats and strategies) and how they are applied in making real world information security decisions. You will also be introduced to how risk management is approached in COBIT 5.

Learning Outcomes

By the end of the unit, you should be able to:

- Critically appraise the principle risk of management in the context of an ISMS
- Understand key concepts behind risk management and how it relates to GRC
- Describe techniques for identifying and prioritising risk and understand the cost benefit approach to risk management
- Describe risk management strategies and their role in establishing controls.

Prescribed Reading

Prescribed reading for this section is noted below, and you will be prompted to read these as you progress through the unit:

- Whitman, M.E., & Mattord, H.J. (2017). *Management of Information Security* (5th ed.).Boston, MA: Cengage. Chapter 6 (Risk Management) and Chapter 7 (Controlling risk)
- Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy,* 9(2), 58-65. DOI: 10.1109/MSP.2010.117
- Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410–430. DOI 10.1108/IMCS-07-2013-0053

7.1 Background and context

Reading: MIS Chapter 6 pp249-253 ("Introduction to risk management")

Risk management is the foundation of security. We will come to a full definition of risk later on but we can say that risks can come from a number of sources. One way of looking at this is the usual split of people, process and technology, but also being aware that (a) external factors can also be a source of risk and (b) the factors can work together to make the risks more significant.

Risk Management - risks diagram

Figure 7.1 Sources of risk

7.1.1 Definitions: what is risk management

Risk is defined in ISO 31000 as "the effect of uncertainty on objectives". The key points to take away from this are:

- There are choices which can be (or have been) made which have an influence on the outcome
- Almost any human endeavour carries some risk, but some are much more risky than others
- Although there are also upside risks (eg managing unexpected success), they do not feature in information security, where risks are always negative
- Potential losses themselves may also be called "risks" – that is, the language around "risk" is often ambiguous. It's important to pay attention to what each author means by the term.

Risk management forms part of the GRC triad – and should be carried out across all an organisation's activities, not just IT or information systems.

7.1.2 Associated concepts

A quick reminder of the key terms from the introductory unit. These also crop up in the Availability Unit.

Asset Something that is worth protecting	Sensitive data, intellectual property, and access to critical operati assets. For example, user credit card numbers are an asset wort in your application.
Vulnerability Weakness that makes a threat possible	As soon as an asset is connected to the outside world, it is vulne challenge is to minimise the vulnerabilities. Vulnerabilities may be because of poor design, configuration mis inappropriate and insecure coding techniques. Weak input valida example of an application layer vulnerability, which can result in
Threat	A bad thing that can happen to your assets. It could be caused b or through an act of nature. Threats can't be managed, though t avoided.

Potential occurrence, malicious or otherwise, that could harm an asset	
Attack (Deliberate) Action that exploits a vulnerability to enacts a threat	Examples of attacks include sending malicious input to an applica flooding a network in an attempt to deny service.

Table 7.1 Key terms

7.2 Identifying risks

Reading: MIS Chapter 6, pp253-273 ("Risk Identification")

Risk management - identifying risks

Fig 7.2 Elements of risk management

This section covers the processes associated with identifying the risks, which is necessary before they can be assessed. This is done through identifying the assets and then the threats and vulnerabilities associated with them as described in the following sub-sections.

7.2.1 Categorising assets

In most approaches to this topic, risks are associated with assets. One of the challenges however is that the term "information asset" covers a wide variety of things. The categories below simply reflect the nature of information systems – people, processes and technology – in a bit more detail.

The obvious assets categories are hardware, networks and software. Many organisations would already have processes in place for identifying and managing these (eg for licencing or maintenance purposes). There are also a number of tools that can be used to enumerate all the assets on a network. Typical details that can be captured are:

- Name
- Owner
- Asset type
- Asset identifier (tag)
- Asset details: eg version, manufacturer, support contract details
- Network location: IP/MAC address, or associated hardware

Other forms of information asset

However, there are other forms of information asset which shouldn't be forgotten. Table 7.1 below summarises them, and how they could be inventoried.

Asset type	Associated inventory data
Data In most cases, the real value is in the data on the system. Many organisations are poor at tracking what data they have, and assessing its sensitivity or value to them (though GDPR and similar laws are perhaps forcing a change here).	Classification (eg sensitivity) Owner Location/size etc Associated Backup/ restore procedures
Procedures How many organisations are aware of what procedures they have, and their vulnerabilities? (You will see in the next unit that the auditors do look for key procedures.)	Purpose Owner Description Related roles and assets
People They are vulnerable to social engineering, and their knowledge of the organisation is valuable.	Base round unique ID (personnel, contractor, customer) Linked to manager/ organisation Linked to roles

Table 7.1 Asset types for risk assessment

Note how all assets have an owner (or line manager!)- this is important for allocated responsibility for risk management. On the other hand, it can be a challenge if an asset or person has more than one owner or manager.

It's important to remember that some assets are more sensitive than others, especially if they involve security of the system: for instance, assets associated with maintaining system security.

Valuing assets

The number of assets can be overwhelming – and it's necessary to prioritise. The obvious way to do this is to focus on the most valuable assets. The problem is choosing a consistent and meaningful way to value them. Accountants are aware of many different ways of valuing assets – Figure 7.3 below summarises some of the options (and the textbook goes into more details):

Figure 7.2 Different valuation models

Figure 7.3 Different valuation models

Although it can be challenging, giving assets a monetary value allows for a common measure across an organisation.

However, it can be difficult for employees to grasp that value (for instance a customer database can be worth millions of dollars), so the value is often communicated using non-monetary values. One example is Data classification (confidential, internal, external) which is easier to explain to staff and relate to security clearance. It is also often easer to think of impact of loss on function of unit/business in terms of bad publicity and days out of action (significance of the organisational units affected).

7.2.2 Assessing Threats

The picture below illustrates why you need to know your assets before you can start assessing threats.

Knowing your assets

Broadly sources of threats can be…

	Deliberate ('attack')	Accidental
Human	Sabotage Theft	Mistakes Illness
Technological	Hacking DDoS	Equipment failure
Natural ('acts of God')	-	

Figure 7.4 Sources of threat: deliberate and accidental

The distinction between deliberate and accidental acts are often blurred. A good example is social engineering (one person's accident can be another person's careless error, and a third's deliberate manipulation).

There are too many threats for an organisation to consider them all. A rough heuristic to getting to a manageable number of issues to consider is:

1. First identify which threats present a danger to this organisation in the current environment

2. Then consider which present the gravest danger now (or in the short term).

Threat modelling

Threat modelling can be used to develop secure code and to secure a system. Threat modelling works to identify, communicate, and understand threats

and mitigations within the context of protecting something of value. There are very few technical products which cannot be threat modelled; more or less rewarding, depending on how much it communicates, or interacts, with the world. Threat modelling can be done at any stage of development, preferably early - so that the findings can inform the design.

Modelling a possible attack can save time, money and other resources for an organisation. Most of the time, a threat model includes:

- A description / design / model of what you're worried about
- A list of assumptions that can be checked or challenged in the future as the threat landscape changes
- A list of potential threats to the system
- A list of actions to be taken for each threat
- A way of validating the model and threats, and verification of success of actions taken

This page gives a brief overview of some approaches to threat modelling

Cyber kill chain

Cyber Kill Chain Has been in use for a few years now[1]. It was developed by Lockheed Martin to help plat to identify and prevent intrusion activity. It is clear and well understood, but is tailored to analysing use of malware and focused on perimeter protection. It is important to be aware of other threats such as social engineering, ransomware, remote access threats too – so it is important to keep on top of current trends.

The model itself has a number of other possible issues[2], for instance:

- The first three stages cannot be managed, so what advantage is there from included them in the model
- The timespans involved can vary from instantaneous to lasting for months and years
- It doesn't capture the importance of pivoting between systems

This is why defence modelling is needed in addition to attack modelling

Unified Kill chain [3]

It is possible to simplify CKC and make it more generic, for instance in the Unified Kill Chain, which highlights the significance of pivoting:

Unified Kill Chain

Another variant focusses on the responses: [4]

Detect Deny Disrupt Degrade

Microsoft's threat modelling

Has created two well known acronyms:

STRIDE: • Spoofing • Tampering • Repudiation • Information disclosure • Denial of Service • Elevation of privilege • Microsoft's original approach to reviewing design level security problems • Characterizing known threats according to the kinds of exploit that are used

DREAD • Damage potential • Reproducibility • Exploitability • Affected users • Discoverability

Microsoft has made much relevant material available, for instance

- Threat Model Analysis and STRIDE [https://msdn.microsoft.com/en-us/library/aa561499.aspx]
- There is a useful threat modelling tool at [https://www.microsoft.com/en-us/download/details.aspx?id=49168]

Other approaches

There many other approaches, including:

- CORAS (Lund, Solhaug & Stølen, 2011). A customized language for threat and risk modelling. Target definition has 3 defined stages that may require multiple iterations [http://coras.sourceforge.net/]
- Attack defence trees (Kory, Kordy, et al, 2013) http://satoss.uni.lu/members/piotr/adtool/ ADTree

Defence in depth

The threat modelling process also includes defences. Ideally, defences will be found to address each of the attacks identified. Modelling tasks are iterative, and the job is never complete because threats evolve constantly. Systems will be added and removed from the enterprise, and the defence models should be applied to new systems. As an organization grows or moves into different sectors, it may attract different attackers with different capabilities.

Both the new systems and the defence models must be re-evaluated in light of changes. For example, if a system that required a specific firewall rule is removed, the firewall should be updated appropriately.

Conclusion

The threat modelling processes can be summarised through four questions: [5]

1. What are we protecting (building)?
2. What can go wrong?
3. What are we going to do about that?
4. Did we do a good enough job?

Notes

[1] http://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html
[2] http://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810
[3] http://Unifiedkillchain.com
[4] https://nigesecurityguy.wordpress.com/tag/cyber-kill-chain/
[5] https://www.owasp.org/index.php/Application_Threat_Modeling

Scenario development

Identifying threats is not easy. One approach is through scenario development, which combines top-down and bottom-up approaches. Figure 7.5 below illustrates the RiskIT model from COBIT 4.1 (which is also used in COBT 5), but other risk management frameworks such as OCTAVE take a similar approach.

Figure 7.3 Using risk scenarios

Figure 7.5 Using risk scenarios

Source: ISACA Journal 2011, Volume 2. https://www.isaca.org/Journal/archives/2011/Volume-2/Pages/IT-Scenario-Analysis-in-Enterprise-Risk-Management.aspx

7.2.3 Assessing vulnerabilities & TVA worksheet

Once there is a ranked list of significant assets and the significant threats associated with them, it can be organised in what Whiteman & Mattord call the TVA (threats, vulnerabilities & assets) worksheet – the aim of which is to identify all possible vulnerabilities:

Figure 7.4 The Threat, Asset, Vulnerability crosstab

Figure 7.6 The Threat, Asset, Vulnerability crosstab

The cross-tab is used to identify the threat/asset combinations that yield significant vulnerabilities. It also identifies where there are unlikely to be vulnerabilities that need to be considered:

Asset:	Asset 1	Asset 2	Asset 3	…
Threat 1	Vulnerability A1T1	x	x	
Threat 2	x	x	x	
Threat 3	x	Vulnerability A2T3	Vulnerability A3T3	
:				*etc*

Figure 7.7 The Threat, Asset, Vulnerability crosstab

It is easy to see that this can generate a significant number of vulnerabilities to consider. The challenge is to narrow the list down to a manageable number.

Self-Assessment Questions

Now try the following.

SAQ 7.1

An evaluation of the threats to information assets, including a determination of their potential to endanger the organization is known as which of the following?

Select one:
- a. threat assessment
- b. risk analysis
- c. data classification scheme
- d. risk identification

SAQ 7.2

Only the InfoSec and IT communities have a role to play in the management of risks to information assets. True or False?

Select one:
- True
- False

SAQ 7.3

The simplified risk management components consist of which of the following groups?

Select one:
- a. People, planning, technology
- b. Planning, performing, tasking
- c. Preparedness, planning, and technology
- d. People, process, and technology

SAQ 7.4

Which term below defines the identification and assessment of risks and also defining acceptable levels of risk within an organization?

Select one:
- a. Risk assessment
- b. Risk analysis
- c. Risk identification
- d. Risk management

Reflective Exercise 7.1

Now try the following.

RE 7.1

Device categorisation

Categorization of assets can be difficult.
One example is a server that has multiple roles and stores multiple different information assets (database, file server, etc) and can therefore have multiple stakeholders or managers. Write notes on how such a responsibility for security could be shared.

Can you think of examples in your own experience?

7.3 Assessing risks

Reading: MIS Chapter 6, pp273-281 ("Risk assessment and risk appetite")

Once risks have been identified, they need to be assessed so that effort can be focussed on the most significant risks.

Figure 7.5 Assessing Risk

7.3.1 Calculations 1: Likelihood, impact

A common model defines risk pseudo-mathematically as:

> The likelihood that the threats to an asset will result in an adverse impact
>
> *Multiplied by*
>
> The consequences (or level of impact) on the value of an asset as a results of a successful attack
>
> *Less*
>
> The percentage of risk mitigated by current controls
>
> *Plus*
>
> The degree of uncertainty of current knowledge of the threat/asset environment
>
> (Whitman & Mattord, 2016, p. 273)

Likelihood may be known (eg actuarial tables), or may need judgement (eg malware attack – in which case the process should be documented). It can be expressed as fraction or %age, but it is often reduced to qualitative measures such as High, Medium or Low.

Impact often focuses on potential loss as it's most straightforward to gather. Impact depends on the organisational context.

> For example, loss of HR for a week may have high impact on them, but the organisation will be able to carry on for a while… so long as the payroll is OK at least.

continued

One approach to understanding the sources of likelihood and impact can be found on one well known application security website:

Figure 7.6 OWASP Risk Rating Methodology - sources of risk

Figure 7.8 OWASP Risk Rating Methodology - sources of risk
Source: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

It is worth comparing this to the *Well-formed risk statement* in the Microsoft Risk Management Approach (Whitman & Mattord, 2016, p.619). Note how the Microsoft approach explicitly considers mitigations, but does not consider the threat agent.

7.3.2 Managing risk / risk appetite

The goal of risk management is not risk elimination: it is risk minimisation, leaving the organisation with residual risk. The aim is to reduce residual risk to match the organisation's risk posture or appetite:

Fig 7.7 Risk minimisation

Fig 7.9 Example risk postures

Self-Assessment Questions

Now try the following questions on risk calculation.

SAQ 7.5

The overall rating, or numerical value, of the probability that a specific vulnerability will be exploited is known as which of the following?

Select one:
- a. Risk
- b. Risk determination
- c. Likelihood
- d. Qualitative assessment

SAQ 7.6

The TVA worksheet is a combination of a prioritized list of assets and their vulnerabilities, and a list of prioritized threats facing the organization based on a weighted table. True or False?

Select one:
- True
- False

SAQ 7.7

Which of the following uses categories instead of specific values to determine risk?

Select one:
- a. Qualitative assessment
- b. Risk determination
- c. Likelihood
- d. Risk appetite

SAQ 7.8

What is the formula for calculating risk?

Select one:

- a. (value * likelihood) – risk mitigated + uncertainty = risk
- b. (value * risk mitigated) + likelihood – uncertainty = risk
- c. (value * uncertainty) + likelihood – risk mitigated = risk
- d. (likelihood * uncertainty) + risk mitigated – value = risk

SAQ 7.9 Risk approaches

Take a few minutes to think of one example of an organisation which would take each of these approaches: minimalist, balanced or conservative.

7.4 Risk control strategies

Reading: MIS Chapter Ch 7: pp307-316 ("Recommended risk control practices")

Fig 7.8 Risk control

Once the risks have been identified and ranked, it is now possible to decide what to do about them.

7.4.1 Different strategies

There are four or five risk management strategies which can be summarised as follows:

Strategy & aim…	Achieved through…	Notes
Defence (also known as **avoidance**): Prevent exploitation of vulnerability	• Application of policy • Training and education • Countering threats • Technical security controls	This strategy in practice is used alongside mitigation.
Transference Aim: Shift the risk to other organisations	Through actions including insurance, outsourcing or sharing (part transference).	Transference inherently creates new (but hopefully lesser) risks.
Mitigation Aim: Reduce the damage caused by exploitation of vulnerability	• Incident response process • Disaster recovery • Business continuity	Incident Response is a key topic which is covered in its own right in Unit 8.

Termination Aim: Remove the source of risk	Removing or discontinuing the asset (Abandoning support would be acceptance)	Similar to avoidance. Can make sense if controlling the risk is more expensive and the asset does not offer value. Related to risk appetite.
Acceptance Aim: Bear the cost	Choosing to do nothing to prevent or contain the risk	Related to risk appetite. This needs to be a conscious choice, not an avoided decision. Can make sense if controlling the risk is more expensive – that is, acceptance is most likely for lower-ranked risks.

Figure 7.10 Risk management strategies

Deciding between strategies

The key point is for management to decide what costs the business can bear, and decide on the risk control strategy appropriately. Costs can include the impact of risk control on your business: At what point are users prevented from doing anything?

One rule of thumb for approaching risk management is given in the text book.

- When a Vulnerability (Flaw or Weakness) exists in an important asset—Implement security controls to reduce the likelihood of a vulnerability being exploited.
- When a Vulnerability can be exploited—Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent the occurrence of an attack.
- When the attacker's potential gain is greater than the costs of attack—Apply protections to increase the attacker's cost or reduce the attacker's gain by using technical or managerial controls.
- When the potential loss is substantial—Apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

(Whitman & Mattord, 2016, p. 296)

Self-Assessment Questions

Now try the following on risk control strategies.

9. Which risk control strategy focuses on planning and preparation to reduce the damage caused by a realized incident or disaster?

Select one:
- a. Mitigation
- b. Termination
- c. Transference
- d. Acceptance

SAQ 7.10

An example of using the transference risk control strategy would be to outsource the security of an asset to another organization. True or False?

Select one:
- True
- False

SAQ 7.11

Which of the following is NOT one of the three types of plans included in a mitigation risk control strategy?

Select one:
- a. Incident response (IR) plan
- b. Disaster recovery (DR) plan
- c. Business continuity (BC) plan
- d. Risk control plan (RC)

SAQ 7.12

When is the acceptance risk control strategy NOT an acceptable approach?

Select one:
- a. The cost of protecting an asset is more than the asset is worth
- b. The asset consists of employee and / or customer information
- c. The asset is considered expendable
- d. The asset has relatively little risk

SAQ 7.13

Which risk control strategy approach can also be referred to as an avoidance strategy?

Select one:
- a. Termination
- b. Acceptance
- c. Defence
- d. Transferral

Reflective Exercise 7.2

Now try the following.

RE 7.2

Write notes on the use of an acceptance risk control strategy. When should such a strategy be used, and why should it not be used for all risks? (and when does it happen in practice – are there any examples in your organisation?)

Self-Assessment Questions

Now try the following questions on risk calculations.

SAQ 7.14

Which of the following can be calculated using the values from an ARO multiplied by the values from an SLE?

Select one:
- a. Cost benefit analysis
- b. Asset valuation
- c. Annualized loss expectancy
- d. Operational feasibility

SAQ 7.15

Asset valuation is the process of assigning financial value or worth to each information asset. True or False?

Select one:
- True
- False

SAQ 7.16

Operational feasibility, which refers to user acceptance and support, as well as management acceptance and support, is also known as which of the following?

Select one:
- a. Organisational feasibility
- b. Behavioural feasibility
- c. Technical feasibility
- d. Political feasibility

SAQ 7.17

Which risk management technique relies on a group evaluating, rating, and ranking assets?

Select one:
- a. Delphi technique
- b. OCTAVE methods
- c. Microsoft's technique
- d. FAIR

SAQ 7.18

What is the easiest way to calculate the cost-benefit analysis (CBA)?

Select one:
- a. CBA = ALE(postcontrol) – ALE(precontrol) + ACS
- b. CBA = ALE(postcontrol) – ALE(precontrol) – ACS
- c. CBA = ACS(precontrol) – ALE(postcontrol) + ALE(precontrol)
- d. CBA = ALE(precontrol) – ALE(postcontrol) – ACS

Self-Assessment Question 7.19

Now try the following (The costs are unrealistic - but that should not stop you being able to answer the questions). There are 10 different scenarios - we suggest you attempt 5 of them at least, to make sure you have grasped the principals.

SAQ 7.19

Table 1 summarises the threat categories faced by a software development company.

1. Calculate and record the ARO (annualised rate of occurrence) and ALE (annualised loss expectancy) for each threat category.

2. Discuss and note how the company could come up with figures for SLE and frequency of occurrence.

You can download a Word version of the table here: Table 1

<object type="text/html" data="https://moodle.napier.ac.uk/repository/draftfiles_manager.php?action=browse&env=editor&itemid=519554958&su height="160" width="600" style="border: 1px solid #000;"></object>

Table 2

Table 2 shows the situation if a number of controls were to be applied.

1. Note where the changes are: what could explain the changes? How can some affect FoO and other the SLE?

2. Using the information in the table and from (1) above, calculate the post control ARO and ALE each threat category.

You can download a Word version of the table here: Table 2

7.5 Control practices: Why simple calculations aren't enough

Reading: MIS Ch 7 287-316 ("Risk management: control risk") (pp307-316 is optional)

There are any number of risk management models that can impact on InfoSec planning. In general anything that's about managing anything should have a risk management model. You are not expected to learn specifics, but some examples you may have come across include:

- COBIT
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- NIST 800-30
- AS/NZS 4360-2005
- ITIL
- CRAMM
- PRINCE2

The appendix in the textbook (pp611-623) gives details of two approaches. What all have in common is a model process. Another example can be found in ISO27005.

Fig 7.9 ISO27000 model of risk control practices
(Source: Everett, 2011)

Fig 7.11 ISO27000 model of risk control practices (Source: Everett, 2011)

Fenz & Ekelhart (2011) includes a review and comparison of several models, and come to a consensus model of five phases:

1. System characterisation
2. Threat and vulnerability assessment
3. Risk determination
4. Control identification
5. Control evaluation and implementation

Reflective Exercise 7.3

Now try the following.

RE 7.3

Research the economic and non-economic impacts of the exploitation of vulnerability. For example, the security breaches experienced by Target in 2013 (or TalkTalk in 2015, or the NHS in 2017).

End of Unit Summary

This unit was structured to build your understanding and awareness of risk management. Learning activities were geared to help you critically reflect upon the practical and theoretical issues associated with establishing risks, responding to them, and to link this to your own work experiences and practice.

In summary, risk management is the process of setting risk tolerance, identifying potential risks and associated impact and then prioritising actions based on business objectives and risk tolerance. The diagram below summarised the concepts covered in this unit.

Fig 7.10 How the elements of risk management relate

Figure 7.12 How the elements of risk management relate.

If you feel ready you should now attempt the End of Unit Progress Test for Unit 7

Further Reading

Risk management:

- Everett, C. (2011). A risky business: ISO 31000 and 27005 unwrapped. *Computer Fraud & Security*, *2011*(2), 5-7. DOI: 10.1016/S1361-3723(11)70015-X
- MIS Appendix: pp611-623 - The OCTAVE Method of Risk Management, Microsoft Risk Management approach
- Microsoft Security Risk Management Guide (from 2004): http://technet.microsoft.com/en-us/library/cc163143.aspx

Threat modelling:

- Al-Mohannadi, H., Mirza, Q. K., Namanya, A., Awan, I. U., Cullen, A. J., & Pagna Disso, J. F. (2016). Cyber-attack modeling analysis techniques: An overview.

Before you leave this unit

When you have completed this workbook please save your work by clicking on the **Submit All Answers and Finalise** Workbook button below. You can now move on to Unit 8 Availability and incident handling