12

Continual improvement

This chapter outlines what is meant by continual improvement and looks at how to initiate processes and activities to achieve it. It forms part of Stage 4 – Performance, evaluation and improvement in the Toolkit Route map.

Key topics

- **What is continual improvement?**
- **How to identify opportunities for improvement**
- **How to create an improvement plan for your organisation**

12.1 What is continual improvement?

Making improvement an objective from the outset will improve both efficiency and security.

Organisations should aim to continually improve the suitability, adequacy and effectiveness of their established ISMS. This does not mean simply fixing problems as they occur, or even that risk must be continually reduced (which may not be possible). Instead, continual improvement requires measuring the effectiveness and efficiency of technology, people and processes and adapting to inevitable changes in the environment – technical, organisational or otherwise. It can be seen as "closing the loop" between risk management and actual incidents.

Continual improvement may therefore be achieved by a number of means, including:

- maintaining suitability of controls to maintain an appropriate level of residual risk in a changing environment (i.e. evolving as technology, threats, assets and vulnerabilities change)
- improving efficiency of the ISMS and controls in meeting security objectives; and/or
- improving the effectiveness of the ISMS and controls in meeting security objectives.

Continual improvement needs to be promoted by leadership and commitment of management and should be included in policy, planning and resources. Implementing a continual improvement process will help an organisation create prioritised and cost-effective improvements that are aligned to business requirements and available resources. Resulting monitoring and reporting capabilities will then increase the potential to identify further opportunities for improvement.

The process for continual improvement should be defined and overseen by the information security function within the organisation. The process should be integrated into existing procedures and processes where possible, so that existing process managers will be responsible for implementing the continual improvement process within their respective area.

12.2 Processes for improvement

Continual improvement involves long-term thinking, implementation of controls or fixes and regular review, monitoring and measurement of people, processes and technology.

Among the many frameworks for continual improvement are COBIT, the Deming cycle and ITIL:

- The Deming cycle is a method for continual improvement, characterised by the Plan-Do-Check-Act iterative steps
- The ITIL set of practices for IT service management defines a seven-step improvement process.

One example of how these processes might relate to continual improvement of an ISMS is given below:

Table 6 - Sample mapping of Deming cycle to ITIL 7 step process

Deming Cycle	ITIL Seven Step Process	Example activities
Plan	1. Define what you should measure 2. Define what you can measure	Identify technical, operational and strategic goals Scoping Risk assessment and risk treatment plans Identify the strategy for improvement Define what you will measure
Do	3. Gather the data 4. Process the data	Implement improvement plans Implement controls, services monitoring etc.
Check	5. Analyse the data	Analyse gathered data (e.g. from monitoring) Carry out gap analysis Internal and external audits
Act	6. Present and use the information 7. Implement corrective action	Implement corrective actions and fixes; Record lessons learned Feed back and report

12.3 Types of improvement

Improvements can be short or long term, and may arise as a result of planned or unplanned events. For example, improvements in the organisation's ISMS may be planned over a period of months or years as part of an overall maturity improvement plan. Alternatively, improvements can be implemented as vulnerabilities and incidents are discovered.

Improvements can be broadly divided into three categories:

- improvements in strategy (i.e. why things are done)
- improvements in practice (i.e. what is done)
- improvements in process (i.e. how things are done).

Improving strategy improves or maintains the suitability of an ISMS in an evolving world and therefore requires improving knowledge and understanding of the environment and threat landscape.

Improving practice (i.e. what the organisation chooses to do, rather than what its members do) can increase the effectiveness of the ISMS and resulting security controls.

Improving processes can increase the efficiency of controls and surrounding processes.

In reality, there is considerable overlap since, for example, improving strategy may result in an increase of both effectiveness and efficiency. Examples of these types of improvement and their effect(s) are given in the table below:

Table 7 - Types of improvement

Type of improvement	Primary improvement	Examples
Strategy	Suitability	• Adjusting strategy and/or security requirements • Creating risk treatment plans • Designing maturity improvement plans • Improving sources of information (e.g. implementing monitoring and detection) • Training and information gathering
Practice	Effectiveness	• Implementing vulnerability fixes • Implementing new controls • Implementing new services • Implementing new processes and organisational structures • Reacting to new opportunistic for bonus improvements • Ceasing unnecessary actions • Implementing an awareness programme
Process	Efficiency	• Refining processes • Renewing technology (e.g. hardware replacement cycles, software updates) • Organisational changes

12.4 Steps in an improvement process

Improvements can be made in the short or long term. However most improvements will follow the process below:

- Identify opportunity for improvement.
- Identify root cause (as applicable).
- Allocate responsibility for implementing change.
- Identify, analyse and evaluate (based on cost vs benefit) possible solutions.
- Plan implementation of changes.
- Implement changes.
- Measure effectiveness of actions (Chapter 10, Measurement for more information on measuring effectiveness).

12.5 Sources of information and opportunities for improvement

Continual improvement therefore involves identifying and reacting to opportunities for improvement. The following table lists a number of potential opportunities for improvement along with potential sources of information associated with these improvements.

Table 8 - Sources of improvement opportunities

Opportunity for improvement	Sources of information
Organisational changes	• Meetings with top management • Departmental/organisational announcements, news bulletins etc.
Changes in business requirements/circumstances	• Third party requirements • Public media and news • Security/business conferences • Team meetings • Management reviews • Service reviews
Change in security requirements	• Policy reviews • Information security incidents • Service requests • Change requests • Bulletins and announcements
Changes in regulatory environment	• Notifications from suppliers • Notifications from third parties • Notification from statutory bodies e.g. the Information Commissioner's Office • Internal security forums • Security mailing lists
Contact with Special Interest Groups	• Security conferences and community meetings • Security mailing lists
Changes in skillsets	• Recruitment of new staff • Knowledge gained from training
User/customer engagement	• Service requests • User satisfaction surveys • Knowledge bases
Service requests	• Service desk management tools • Knowledge bases
Risk assessments	• Risk assessment outputs • Gap analysis reports
Vulnerabilities	• Vendor vulnerability announcements • Security community mailing lists • Results from penetration testing and vulnerability scanning • Log files • Service requests and notifications from users/customers
Information security incidents (see also Chapter 11, When things go wrong: nonconformities and incidents)	• Intrusion detection/prevention system alerts • Log files and network flows • Knowledge gained from analysing and resolving incidents
Internal audit and review (see also Chapter 11, When things go wrong: nonconformities and incidents)	• Review meetings • Policy reviews • Audit reports • Vulnerability scanning and penetration testing reports • Security reviews
External audits	• Review meetings • Audit reports • Vulnerability scanning and penetration testing reports • Security reviews

12.6 Improvement as part of ISMS formalisation

Where an organisation's ISMS is not yet ISO/IEC 27001 compliant, and the organisation wishes to reach this level of maturity, it should treat the process as a standard project or programme.

Following the ITIL continual service improvement approach, organisations can create an improvement plan by considering the following:

- What is the vision?
- Where are we now?
- Where do we want to be?
- How do we get there?
- Did we get there?

In order to consider the vision for improvement it is important to understand the level of resources available and achieve the support of top management.

12.6.1 Vision for improvement

Organisations may wish to consider:

- Who will provide ownership and direction for information security improvement?
- Where does information security report within the organisation (i.e. level of seniority)?
- How quickly does the organisation wish/need to change?
- How much resource can be made available?
- What is the scope and remit of the improvement programme?
- How can goals be made specific, in order to provide clear directing and measurable targets?

12.6.2 Where are we now?

To measure its current level of maturity of information security, the organisation can carry out benchmarking and comparisons with similar organisations. This can give an indication of relative maturity and help to prioritise certain work areas.

Assessment may also be carried out via self-assessment, internal or external audit. Self-assessment can be a useful tool, but involves time and effort from internal staff, and the level or assurance may not be as great as that provided by a more formal audit. However, this will often be an appropriate starting point for an improvement process. External audits may provide more assurance and act as a greater catalyst for improvement, but can be more costly.

12.6.3 Planning and implementing (where do you want to be and how to get there)

Once the organisation has analysed its current state and compared it to its desired state, the results should be documented and compared in a gap analysis, which will form the basis of the improvement programme.

The gap analysis will provide the objectives for the improvement programme, which should be prioritised according to business requirements and an assessment of how much effort is required. Certain objectives might provide the opportunity for "quick-wins", which can be useful to improve buy-in and demonstrate progress, whereas other activities may need long-term projects to achieve. Benchmarking against similar organisations can also prove to be useful during the prioritisation process.

Improvement plans for identified activities can then be planned in an incremental manner to increase the overall level of maturity in a measurable way. For example, in planning to improve awareness of individuals across the organisation, where the organisation has identified that it needs to train everyone annually, the following stages might provide observable milestones:

Table 9 - Simple maturity model for awareness activities

Level of maturity	Milestone
Low	Information security awareness training is available to all users within the organisation.
Medium	Information security awareness training is compulsory for all users within the organisation and is repeated on an annual basis
High	Information security awareness training is compulsory for all users within the organisation, is repeated on an annual basis, and awareness is tested and measured by such means as spot checks, incident simulations, tests etc.

12.7 Measurement

In order to determine whether or not goals have been achieved, appropriate measurements should be used (see Chapter 10, Measurement, for further information).

Summary

- The goal of continual improvement is to iteratively identify and implement ways to make an established ISMS more cost effective and appropriate
- Improvement activities are also necessary during the creation of an ISMS
- Continual improvement can include adapting to the current environment, or improving the efficiency of controls and/or processes
- Continual improvement should be an objective from the outset when implementing any ISMS

Resources

No resources.

Reading list

No items.