Common ISO 27001 Gaps

By Bil Bragg – ISSA member, UK Chapter

Based on a review of 20 gap audit reports for a variety of organizations, this article should help your organization if you are considering ISO 27001, or wish to ensure you comply with best practice.

Abstract

Companies considering getting certified to the international information security standard ISO 27001 often commission a gap audit to find out what they are missing at a high-level. Many of these gap audits have common areas that are not yet in place, such as reviewing user access rights and security in supplier agreements. This article should help your organization if you are considering ISO 27001, or wish to ensure you comply with best practice.

This article is based on a review of 20 gap audit reports for a variety of organizations, including public sector organizations, global enterprises, financial, manufacturing, and technology companies. Most organizations have many of the controls in place already, such as security in Human Resources, password management systems, and physical security controls. However, these audits show that many of the organizations shared gaps in their information security controls. This is certainly not an exhaustive list of gaps, but it may help give you an understanding of the broader requirements of implementing an Information Security Management System (ISMS).

The references in parentheses refer to "Annex A: Controls and Objectives" in the ISO 27001:2005 standard and the section reference in the code of practice ISO 27002:2005.

Common System Gaps

4.2 – Establishing and managing the ISMS

ISO 27001 has basic structural requirements for an ISMS. These include what you want to have in your ISMS (the scope) and a risk assessment.

Few organizations had a formal statement of scope (4.2.1(a)) but often had a good idea of what would be in scope of the ISMS. For larger organizations this is usually a department, service, or location such as the IT Department or a Data Center; whereas smaller organizations usually include the whole organization. Where the scope is a part of the organization, it is important to define it in order to understand where the boundaries are and what is included and excluded from the scope.

The risk assessment is a key part of an effective ISMS (4.2.1(c)-(h)). Many organizations had a form of risk assessment. However, in most cases it did not meet the specific requirements of the standard. Generally, existing risk assessments either did not consider assets first, did not consider all important assets in scope, or did not consider impacts to confidentiality, integrity, and availability. Often, the risk assessment methodology was not documented along with criteria for accepting risk.

It is not surprising that at the gap-audit stage, many ISO 27001-specific requirements are not in place, but they are worth mentioning. Following on from the risk assessment, management should approve the proposed residual risks; the organization should implement a risk treatment plan (4.2.2) and produce a corresponding statement of applicability (4.2.1(j)).

6.0 – Internal ISMS audits

Only one organization had an internal ISMS audit program, and none of the organizations had undertaken a management review of the ISMS. Many organizations had an internal audit function that covered IT and some compliance requirements such as Sarbanes Oxley, so less work would have been needed for those to meet the requirements. Organizations with a Quality Management System would be able to extend their existing internal audits and management reviews to cover the requirements of ISO 27001.

A.6 – Organization of information security

A.6.1 Internal organization

Objective: To manage information security within the organization.

An information security committee or forum that would meet regularly was not yet in place (A.6.1.1), more so for smaller organizations. This is best practice rather than a specific requirement; however, implementing and running an

ISMS is difficult without this. Additionally, a staff member had not been formally assigned an ISMS manager-type role (A.6.1.2). These would be key to getting an ISMS up and running. Often organizations have existing regular management meetings that can be extended to include the ISMS.

A.6.2 External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

Identifications of risks relating to suppliers and customers were generally sporadic or not in place (A.6.2.1). Many organizations use suppliers with logical or physical access, such as IT support companies, security guards, and cleaners or provided systems access to customers. Following on from this, agreements with these suppliers and clients (A.6.2.3) that have access to important information assets did not include key provisions such as an information security policy, asset protection, staff screening and training, access control policy, reporting security incidents, monitoring and auditing, service continuity arrangements, and use of subcontractors.

Many of the smaller organizations outsourced IT functions, which gave these IT support companies full access to their information. Although there was a high level of trust for these companies and individuals supporting them, there had been no formal risk assessment and no agreement with the expected information purity provisions.

A.7 – Asset management

A.7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

The standard requires an inventory of all important assets (A.7.1.1). Many organizations had an inventory of hardware assets maintained by the Finance department. Some IT departments also had software inventories through using discovery tools. The standard requires an inventory of important assets that typically includes non-physical and information assets such as systems, databases, documentation, services, people, and intangibles such as reputation. These assets would also be used in the risk assessment.

A.9 – Physical and environmental security

A.9.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

Many of the gaps in physical security were specific to the organizations. However, most if not all should be identified as part of the ISMS risk assessment. Common examples of these were CCTV cameras that were obscured or not working, and fire doors used as normal doors, which meant that locks were broken or ineffective, or the fire doors were often wedged open.

A.10 – Communications and operations management

A.10.7 Media handling

Objective: To prevent unauthorized disclosure, modification, removal, or destruction of assets, and interruption to business activities.

There was a widespread lack of any formal procedures for media handling and media disposal (A.10.7). This would include use of USB flash memory sticks, external hard drives, DVDs, and printed media. Often, where organizations issued USB flash memory, there was no requirement for encryption or restriction on the use of personal USB flash memory.

As expected, smaller organizations tended to have no media handling policy whereas larger organizations did, but with no procedures that would meet the requirements. For example, one large organization used a company to destroy hard disks, but this was not formally recognized.

A.10.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

Many organizations did not have an information exchange policy (A.10.8.1) for how to send confidential information over email, for example, whether to send confidential information at all, or use a specific level of encryption. Related to this, many organizations did not have agreements with customers or suppliers on how to exchange confidential information (A.10.8.2).

One small company received regular, confidentially classified information from a large financial institution via email. Despite how hard the company tried, the financial institution was not willing to agree to send the information encrypted! On the whole, most organizations did tend to encrypt information that individuals determined as confidential, using ad hoc means of encryption, rather than based on a company-wide policy.

A.10.10 Monitoring

Objective: To detect unauthorized information processing activities.

Clocks on Microsoft Windows servers and desktops on the internal network were generally synchronized with a public NTP server (A.10.10.6); however, servers in DMZs, CCTV systems, and some network devices were often not synchronized. Most organizations did not know if clocks on servers and network devices not on the internal network were synchronized. Date and time stamps for audit logs are important when troubleshooting and may hinder the credibility of using audit logs as evidence if inaccurate.

One smaller organization had desktops that synchronized with a domain controller, but the domain controller did not synchronize with an external time source. Two organizations had CCTV system clocks that were out by over 10 minutes.

A.11 – Access control

A.11.1 Business requirement for access control

Objective: To control access to information.

Most organizations had an access control policy that was inferred for each system through the way Active Directory was configured, or the way roles within an application were setup (A.11.1.1). The standard requires a documented access control policy that identifies common roles for each business application. The access control policy should specify rules ensuring the concept of least privilege.

All organizations tended to have well-defined Active Directory groups and applications with well-defined roles with owners (sometimes informal) responsible for access authorization. Smaller organizations on the whole did not have an access control policy, whereas larger organizations mostly had a very high level access control policy without specifying systems or roles.

A.11.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

Most organizations did not have an effective, regular review of user access rights (A.11.2.4). Reviews of access rights were usually ad-hoc, and only covered a few systems such as Active Directory and the core business applications, rather than a formal review across all systems. Larger organizations were more likely to have a regular review of user accounts for Active Directory and the main applications. For those that did not have a formal regular review of access rights, a sampling of different operating systems, databases, and applications showed old active test accounts, accounts for people who had left, and generic accounts for which the purpose was unclear.

A.11.3 User responsibilities

Objective: To prevent unauthorized user access and compromise or theft of information and information processing facilities.

Many of the less obvious systems had accounts with very weak or default passwords. These included network devices, databases such as Microsoft SQL Server and Oracle, physical access control systems, and local accounts on older servers (A.11.2.3 and A.11.3.1). For example, one large organization had a physical access control system with a default administrator password, and another large organization had an SQL Server database with a blank 'sa' password.

Although most organizations had clear desk and clear screen policies (A.11.3.3), multiple breaches of these policies were often observed, most often by screens left unlocked with staff away from their desks.

A.11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

Some organizations had effective technical controls for mobile computing and teleworking (A.11.7.1 and A.11.7.2), such as encrypted hard disks for laptops, encrypted smart phones, two-factor authentication for VPNs, and endpoint protection. The gaps found in the majority of organizations were that a formal policy for mobile computing should be in place and that a policy and procedures for teleworking is needed. These should include physical protection, rules, and advice for connections used in public areas, and possible access by friends and family.

As a typical example, one organization had a procedure for assigning laptops and blackberries, which included an agreement by the staff members that they would look after them. The organization also enforced some security controls for remote access and hard disk encryption. However, there was no guidance on how staff should protect information on the assets.

A.12 – Information systems acquisition, development and maintenance

A.12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity, or integrity of information by cryptographic means.

Many organizations did use cryptography to protect emails, information on removable media, and laptop hard disks (A.12.3.1). However, there was generally no central policy that ensures a consistent management approach that ensures appropriate levels of encryption through risk assessment, and that ensures that keys and passwords are protected and recoverable.

Examples of cryptographic controls in use even without a policy were two-factor authentication for VPNs, a variety of full-disk encryption software products for laptops, PGP encryption for emails, and e-wallets for password storage.

Some of the organizations used external companies for outsourced software development (A.12.5.5). In many cases contracts did not stipulate who had the intellectual property rights of the code, escrow arrangements in case of dispute or business failure, requirements for quality and security functionality of the code, or a right to audit the company. In one example, some of the code was copyrighted to the organization and the rest of the code was copyrighted to be external company, even though the code was only used by the organization.

Many organizations had effective technical vulnerability management (A.12.6) for Microsoft, Linux, and database software but did not manage vulnerabilities for some other software in use, especially on desktops, such as Adobe Reader and Adobe Flash. A typical example was that existing publicized vulnerabilities in Adobe Reader had not been considered as a possible vulnerability. A check on the desktop estate showed that there were many older versions of Adobe Reader with no central configuration management.

A.13 – Information security incident management

A.13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Many organizations did not have a formal procedure for reporting security events (A.13.1.1), nor a mechanism to ensure that types, volumes, and costs of information security incidents could be quantified and monitored. For example, a sample of staff members was not clear on what a security event was and how it would need to be reported.

A.14 – Business continuity management

A.14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Some organizations did not have a business continuity plan (A.14.1). For those that did, it was generally a bit dusty. Current business processes should be assessed to determine acceptable maximum downtime and business continuity plans created to ensure business processes can be back in place within that time frame, given a variety of scenarios.

Most organizations that had business continuity plans did not test them regularly or with a wide enough coverage (A.14.1.5). For example, in one case the only test was that backup tapes were restored to a remote location. A variety of techniques and scenarios should be used to give assurance that plans will operate in real life.

A.15 – Compliance

A.15.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements.

All organizations had not identified all applicable legislation within the scope of their ISMS (A15.1.1), such as data protection legislation and computer misuse laws. Organizations had also not established a mechanism to ensure they were kept up-to-date on relevant legislation and regulations.

Conclusion

There are many gaps that organizations have in common in their information security management systems. The most important gap in common is that key staff who would be involved in implementing ISO 27001 had not yet been given training on what ISO 27001 was and how to implement it.

Although many smaller organizations did not have the policies and procedures that the larger organizations had, they still had informal practices that met many of the requirements of the standard that could be formalized. Smaller organizations generally did not have much in the way of incident management or business continuity management. Due to other compliance requirements financial institutions usually had less gaps than others.

Organizations may have these common gaps as it is not obvious that there are significant information security risks until they have been addressed. For example, considering risks to assets such as applications, staff and suppliers, not just hardware assets: all staff being aware of the information exchange policy so that it is less likely that a CD or email is sent containing personal records unencrypted; a regular review of access rights that clears up defunct domain administrator accounts with weak passwords that also allow remote access; and an effective test of business continuity plans that shows how much they need to be updated.

About the Author

Bil Bragg, ISSA member UK Chapter, is a penetration tester with Dionach Ltd and an ISO 27001 lead auditor with Certification Europe. He may be reached at bil.bragg@dionach.com.