ISO 27001:2013 Annex A

ISO 27001:2013 is one of the most highly regarded security frameworks in use today. Used in both the public and private sector, becoming familiar with the recommended controls can be a daunting task. We are here to help break it down.

AN INTRODUCTORY DISCUSSION ON ISO'S RECOMMENDED CONTROLS.

Version History

Version	Revised By	Amendment/Reason	Date
0.1	Adam Miller	Initial draft	25/09/2017
0.2	Adam Miller	Including Introduction and first read through.	30/09/2017
0.3	Adam Miller	Continuing initial read through	13/10/2017
1.0	Adam Miller	Completed read through	20/10/2017

CONTENTS

INTRODUCTION

ISO27001:2013 is a management standard that details how the setup an Information Security Management System(ISMS) in an organization. What this is, is establishing a blueprint of policies, standards, baselines and procedures for information governance, risk, and compliance. It lists controls we must follow as requirements for establishing, implementing, operating, monitoring, reviewing, managing, and continually improving the ISMS. These controls that are listed in the annex of the standard, and discussed in great detail in ISO 27002, are tailored to your organization and some may be removed if not relevant. For example, if your organization does not develop software, you can remove controls related to software development. This allows the 27001 standards to be a good fit for any organization.

Before we begin we must understand some things. Firstly, there is a lot of overlap between 27001 and 27002 ISO standards. ISO 27001 tells us what we need to do to gain certification. ISO 27002 explains exactly how to implement the ISO 27002 controls. ISO 27001 can be split into two parts. The first part is the initial 10 clauses outlining the standard and are:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

The second portion is the list of controls in the documents Annex. It is the controls that this document discusses.

The way this document came into existence should also be consider when deciding if it will be of use to you. I recently passed my CISSP exam and decided to study the individual frameworks covered by the CISSP in depth to improve myself. The first framework I wished to tackle was the ISO 27001 as it is so popular and had been referenced in my CISSP studies several times. I wanted to write about what I was learning about to assist my own understanding, and to act as something I could read over in the future. When I was reading through the framework I found the first 10 clauses to be very much a repeat of what I covered in the CISSP and didn't feel a need to write up a document on them but the controls contained in the Appendix captured my imagination.

This document is to act as a bridge between ISO 27001 and ISO 27002. It explains what each of the controls specified in the appendix are for, and the security concepts underpinning them. It does not go into sufficient detail to allow an organization to become certified, but can help with understanding the requirements prior to taking on such an undertaking.

At the very least I hope this document, that I initially envisioned as being no longer than 5 pages helps InfoSec students learn and grow.

SECURITY CATEGORY – 5.1. MANAGEMENT DIRECTION FOR INFORMATION SECURITY CONTROL

5.1.1. POLICIES FOR INFORMATION SECURITY.

Organizations should have written documents, detailing your security policies, standards, guidelines and procedures, and these should be readily accessible to staff and other relevant parties. There are two "levels" of documents you should keep. The first level is the Information security policy which gives a high-level view of our security objectives. It displays the reasoning for our security policies and how they tie into your organizations goals. It describes the security we have and shows that senior management supports the organizations security initiatives, which can be very important for gaining employee compliance. This policy provides direction for an organization, with regards to security, and it may reference regulations, legislation and other lower level organization policies. It should also provide guidance on how deviations to policy requirements are handled by management.

The second "level" includes lower level policies that are simple, easy to understand and highly specific. They may describe Acceptable Use of IT systems and resources, how identity and access is managed, how backups are carried out including what the organizations appetite for data lose is, and how the organization treats personally identifiable information(PII). There can be many policies but they need to be specific in their focus and simple to understand of all employees. Your organization can have dozens of policies if needed, but there are some specifically recommended by ISO in these controls. They are (International Organization for Standardization);

- Access control,
- Information classification,
- Physical and environmental security,
- Acceptable use of resources,
- Clear desk and clear screen,
- Information transfer,
- Mobile devices and teleworking,
- Restrictions on software installation and use,
- Backup,
- Protection from malware,
- Management of technical vulnerabilities,
- Cryptographic controls,
- Communications security,
- Privacy and protection of personally identifiable information,
- Supplier relationships

5.1.2. REVIEW OF POLICIES FOR INFORMATION SECURITY.

Security is a continuous process and writing policies is not the end of what is required for certification. This is not because there may be errors in your latest draft but because security as a landscape is constantly shifting. With new laws, such as the General Data Protection Regulation and Network and Information Systems Directive in the European Union, being introduced and past laws like the EU-US Safe harbour agreement being

invalidated, our policies should be reviewed on at least an annual basis to make sure they are still fit for purpose. TThis will not only keep your organization safe from a regulatory perspective but for changes to the security landscape too, such as the introduction of IoT and wearables devices, allowing our policies to evolve over time to best protect the organization and to ensure best practices can be adhered to.

SECURITY CATEGORY – 6.1. INTERNAL ORGANIZATION

6.1.1. INFORMATION SECURITY ROLES AND RESPONSIBILITIES.

To ensure any tasks discussed in your security policies are fulfilled it is important that roles and responsibilities are designated. This gives accountability and responsibility to ensure duties are carried out.

6.1.2. SEGREGATION OF DUTIES

Separation of duties is one of the most well-known and important IT security tenets. It is a key concept to the CISSP, CISA, Security+ and a variety of other certification and even regulations and laws such as Sarbanes-Oxley act in the United States of America. The control deals with the risks associated with one person having too much power. To give an example of a risk this control deals with; if an employee can both write and sign checks he can easily write out a check to himself and sign it. This is an example of where there is no control in place for the separation of duties. If we were to implement this control in this situation that employee would be able to write a check but would need another employee to sign it. Similar risks can occur frequently in an organization and can impact the organization in a variety of ways, and not just the financial example given. Having controls in place to enforce a separation of duties and having this in policy documents can give us protection and mitigate these types of risks.

6.1.3. CONTACT WITH AUTHORITIES.

Breaches will happen as risk can never be completely eliminated. The organization needs to be prepared for such an event and part of this is having procedures in place with contact information that instructs the staff member in how to contact the relevant authorities. These procedures should contain contact information for who to contact for the relevant breaches, such as contact information for the Data Protection Commissioner for Personally Identifiable Information being stolen, and it should be clearly stated when to contact those authorities. This document should be readily available and staff should be made aware of it.

6.1.4. CONTACT WITH SPECIAL INTEREST GROUPS.

As security is always changing it is important that your specialist staff keep in touch with updates and developments. This can be achieved in many ways such as requiring staff with certifications should keep their membership with the accrediting bodies, maintain their certificate with CEU/fees and and keep in contact with the community. Encouraging staff to attend industry events like OWASP talks and other events, and encouraging staff to keep up to date using news sites, blogs and other resources is also good practice. This not only gives your staff an up-to-date insight into new and developing threats but also allows them to draw on the community, gain mentors and exchange information to better prepare you for defending your organization.

6.1.5. INFORMATION SECURITY IN PROJECT MANAGEMENT.

Whenever we are planning a new project, whether its infrastructure, application, or other, we should always include security into our earliest stages of planning, design, and management. This allows security risks and issues to be identified at the earliest stage of the project, when it is cheapest and easiest to deal with. While we will look for security problems in the project itself, we should also look at new attack vectors that the project being implemented could introduce and the potential risks that could be generated from the result. As described in 6.1.1 defined roles and responsibilities for information security should be established to ensure all staff know their role for a secure project throughout its lifespan.

SECURITY CATEGORY – 6.2. MOBILE DEVICES AND TELEWORKING

6.2.1. MOBILE DEVICES POLICY.

In the modern organization, mobile devices are a given. Staff with laptops that move around and leave your organizations premise, uncontrolled iPads, Smart phones with incredibly accurate cameras and wearables that have Wi-Fi and Bluetooth access, the threat landscape is changing. All organizations big and small face risks from these devices and this needs to be properly managed. This control recommends a Mobile Device Policy that addresses these concerns. This policy should include details on (International Organization for Standardization);

- registration of mobile devices so the organization can track device and identify owners in case of misuse
- physical protection of mobile devices
- restrictions on software installation
- mobile device software versions and for applying patches
- restriction of connection to information services
- access controls
- cryptographic techniques to encrypt the drive and for connecting the office from outside the organization.
- malware protection such as requiring a specific Anti-Virus version with up to date signatures
- remote disabling, erasure, or lockout in case the device is lost so that any sensitive information stored on that device can be destroyed
- backups
- use of web services and apps

With mobile devices, there are times when it is the employee's private property and placing restriction on what the employee sees as their own, can be a challenge but is necessary for the protection of the organization. Having a policy in place that an employee needs to read through and agree to can help staff understand where the boundaries of acceptable use are and the requirements to use a device at all. This easy to understand document can help improve acceptance of the organizations mobile device security.

Even just making an employee aware through security awareness training can reduce the risk of mobile devices such as by making the employee conscious of his or her surroundings when they open sensitive emails and can encourage an employee to question what wireless networks they use for business purposes.

6.2.2. TELEWORKING.

When an organization allows its employees to work remotely it introduces risks that must be acknowledged and mitigated against. There are many things an organization should consider such as whether to provide an employee with equipment to work from home with, or to allow them to use their own personal devices. In general, the organization will provide company laptops to staff working from outside of the organization, who connect to the corporate network with a VPN. Organizations that allow employees to use their personal equipment should take additional steps to ensure threats are not introduced to your network, for example requiring software to be installed that monitors applications installed on the device, granting the corporate IT

team with additional powers over the personal device and ensuring the security level of that device (such as requiring a patched OS, up-to-date antivirus etc).

SECURITY CATEGORY – 7.1. PRIOR TO EMPLOYMENT

7.1.1. SCREENING

Screening of candidates should be carried out prior to them being offered a role at your organization. This has a range of benefits if done in an appropriate manner. These benefits can include confirming an employee's qualifications, work history and finding issues with the person that could compromise their integrity. All screening to be carried out should be executed to a level that is appropriate for the role the candidate is applying for. To ensure the correct screening measures are taken all steps in the process should be defined in a procedure document and executed in a manner that meets local laws and regulations. Some concerns that the organization should address when deciding on screening procedures are; which specific employees/roles will be carrying out the screening, what exactly is screened for and who verifies that the screening process was carried out correctly.

Some examples of what we can screen for are;

- Valid references given when candidate applied for the position,
- Garda/Police vetting where required,
- Gaps in CV,
- Criminal conviction,
- Background in drug, alcohol or gambling abuse,
- Verification of the credentials the candidate claims.

Depending on the industry and role the candidate is applying for the depth of the screening can vary but screening should be carried out for employees, contractors, and outsourcing companies.

7.1.2. TERMS AND CONDITIONS OF EMPLOYMENT.

It is important that information security responsibilities for both employees and contracts are included in their contracts. This can ease confusion as all employees and contractors understand what is expected of them and agree to these terms before joining your organization. These can include confidentiality and non-disclosure agreements for those staff handling sensitive data, they can inform employees of any monitoring that is carried out (within the boundaries of local laws), the use of the employee PII and even acknowledgements that the results and outputs an employee produces within the course of their employment is owned by the company (which would deal with patents, copyrights and other IP types). Lastly it should include general information security requirements and responsibilities.

SECURITY CATEGORY – 7.2. DURING EMPLOYMENT

7.2.1. MANAGEMENT RESPONSIBILITIES.

This control requires we make sure management enforces the information security requirements. Good security practices cannot be put in place and abided by without managerial support. For example, having great, comprehensive password protection policies is no good if a manager allows, or even encourages staff to share login credentials before they go on annual leave so they can cover for each other. Managers must be specifically instructed to apply information security standards as per the organizations policies and procedures, including providing training if required.

7.2.2. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

It is often said that the biggest risk to security comes from staff and users of IT systems. The best defence we have against this weak link is training. Studies have shown that the more educated a user is the less likely they are to be the cause of security incidents. This is due to increased knowledge but also increased awareness of the risks the staff member's organization faces. From this it quickly becomes apparent that one of the best ways to protect your organization is to put into place an initiative for continuous security awareness training, and more general information security training, for all staff. This will ensure that staff understand their responsibilities and also attack types and the different attack/threat vectors. It can even instilling best practices into staff, such as not holding the door open to unidentified people, not giving out information over the phone, to be more scrupulous when deciding if an email is a phishing attack and even to discourage staff from discussing sensitive matters with colleagues in public places. Part of this training should include familiarizing staff with policies and other security documents.

7.2.3. DISCIPLINARY PROCESS.

It is inevitable that, despite our best efforts, there may be times when it becomes necessary to discipline staff. Having a defined disciplinary process that is enforced ensure uniformity and fairness is an essential practice for modern organizations. This flows into ensuring security policies and procedures are followed and disciplining staff for deviations. If there is a verifiable security breach and the cause is found to be a staff member not following best practices security breach the disciplinary process should begin and it should allow for different degrees of result depending on the severity of wrongdoing by the staff. On top of this, employees should be made aware of this process.

SECURITY CATEGORY – 7.3. TERMINATION OR CHANGE OF EMPLOYMENT

7.3.1. TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES.

An organizations security should facilitate ensuring that an employee leave, either through termination or resignation, without negatively impacting the organizations security posture. This presents additional security concerns and challenges. We need to ensure that our IT departments are in sync with our HR departments so that the employee's access to information systems is revoked at the correct time to protect our systems and data from the former employee. Co-ordination is also required to ensure company equipment in the possession of the employee is returned. The employee should also be made aware of any obligations he or she has to the organization after his employment ceases, such as NDA's and non-compete clauses. These steps should be carried out when-ever an employee leaves their role even if they are simply taking up a new role in the same company, as it limits the risk of data breaches and permission, or privilege, creep.

SECURITY CATEGORY – 8.1. RESPONSIBILITY FOR ASSETS

8.1.1. INVENTORY OF ASSETS.

This control is one that is all too often overlooked. How many companies and organizations have a complete list of all their IT assets and those assets owners? Often our inventories grow too large to be managed without additional resources and then become neglected and out of date. This can lead to security risks of lost assets (unowned) sitting on our network waiting to be compromised, new rogue devices getting added to our network and us being unable to distinguish them from our legitimate assets, even from a patch management perspective knowing what you own is essential for security. Any device that is associated with information or information processing should be recorded. We should keep a record of all these assets including documentation for them, license information and contracts/SLAs (for utilities). There are tools that make this task easier and while it is something that can require a dedicated and substantial effort to develop and maintain, it is something that is one of the more essential building blocks to implementing your ISMS.

8.1.2. OWNERSHIP OF ASSETS.

All assets in your organization need to how owners assigned to them. This gives us a point of contact should any issues arise that require further investigation or remediation. These asset owners can log in and take care of the regular maintenance of a system, such as hardening and patching. This record of owners should be included in our inventory list described in the previous step. Knowing who to contact can be vital in timely remediation and damage mitigation during a breach when every second counts. Knowing the owner also lets us know who is responsible for protecting those systems, adding/removing them from our inventory and abiding by the asset lifecycle policies, including correct disposal of the hardware and data when that asset is end of life.

8.1.3. ACCEPTABLE USE OF ASSETS.

No user should have complete, unfettered use of company assets. Having the acceptable use of assets documented in an Acceptable Use Policy and then distributing that to all your employees can help you ensure assets and resources are used in a responsible way. Part of this policy is to ensure assets have an appropriate level of security for the data and function it is used for, this means you can have multiple Acceptable Use Policies, one for each classification level of data housed in the various assets. By reducing misuse of assets by employees, making them aware of and having them agree to this policy we reduce risks being introduced by assets being used for non-business purposes.

8.1.4. RETURN OF ASSETS.

If we don't ensure company owned assets are returned to the company during termination we run the risk of losing control of those assets and, more importantly the data contained within. We also run risks that the assets may be misused or damaged. Human resources and your IT team should liaise prior to termination of employment to ensure any company assets in the control of the leaving staff member are promptly returned to the company. There should also be technical controls in place to ensure that data residing on any personally owned devices of the employee is transferred to the organization.

SECURITY CATEGORY – 8.2. INFORMATION CLASSIFICATION

8.2.1. CLASSIFICATION OF INFORMATION.

Not all data is made equal. Given the high costs in both resource and complexity of more stringent security controls and the unequal value of data it is recommended to take a tiered approach to data management. This simply means dividing data based on some requirement into tiers, with each tier having different security requirements and levels of access. One of the most famous example of this is the United States of America's federal government's data classification levels of Top Secret – Secret – Confidential – Unclassified with the criteria for each listed below from Wikipedia (Classified information in the United States, n.d.);

- Top Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- Information is classified Secret when its unauthorized disclosure would cause "serious damage" to national security.
- Confidential is defined as information that would "damage" national security if publicly disclosed, again, without the proper authorization.
- Unclassified is the default and refers to information that can be released to individuals without a clearance.

Having a well-defined and simple to understand data classification scheme can reduce the effort required when deciding how to secure systems housing the data by giving a baseline of security requirements for that tier.

8.2.2. LABELLING OF INFORMATION.

Having developed your classification plan you now need to ensure all data in your organization is designated a classification and is easily identifiable as being given that classification to avoid accidental disclosure or mishandling. An example of this would be to label media used for storing the data with coloured labels, such as **RED** for top secret, anyone handling the media then knows its classification level at a glance. There should be procedures in place to instruct authors how to correctly classify their outputs. All documents should state their classification level in an easy and quickly understandable way. This labelling effort should be part of your organizations standard process and documented in your handling procedures.

8.2.3. HANDLING OF ASSETS.

This is very important for organizations dealing with sensitive information. There should be clear, documented procedures for how data is handled at the different tiers including how information is stored and transported and who is authorized to handle it. There should also be instructions on how data and media should be destroyed at the end of its life.

SECURITY CATEGORY – 9.1. BUSINESS REQUIREMENTS FOR ACCESS CONTROL

9.1.1. ACCESS CONTROL POLICY.

Access to assets is a key concern for any organization. Access should always be based on the businesses needs and tailored to the specific employee and asset type. Employees need just the right amount of access to perform at their job. Too little access and key functions in an organization may be left unfulfilled. Too much access and the organization may suffer a data breach, tampering of services and outages, either by accident or by malicious intent. The best way to approach access controls, and is the way recommended by ISO, is documentation! This is a reoccurring theme but we need documented process to ensure repeatability, uniformity, and fairness. In this case we should consult with asset owners on what access levels different users, or user roles, require and document them. It is important to ensure we protect both physical and logical access. Restricted SSH access is only so helpful if the server hardware is physically protected.

Keep in mind when granting rights to users that the user must have both the correct security clearance to access that data and a legitimate business need to require it. By keeping these in mind we can avoid granting excessive access to individuals. Periodic reviews can also help us prevent privilege creep as roles and requirements change.

9.1.2. ACCESS TO NETWORKS AND NETWORK SERVICES.

This is similar to the above control but where 9.1.1 focuses on access to assets, 9.1.2's scope is focused on network access. Best practice for access control should expand to the entire network, not just the assets. This policy should specify which networks and services should be accessible with authorization and authentication procedures for access, consideration for workers accessing the network from public areas using VPN or Wi-Fi and monitoring requirements should all be detailed. Consider segmenting your network into separate areas with VLAN's, DMZ's or similar to control network access between different areas of your organizations.

SECURITY CATEGORY – 9.2. USER ACCESS MANAGEMENT

9.2.1. USER REGISTRATION AND DE-REGISTRATION.

This control details how our organization onboards new employees and disables the accounts of former employees. The process should be formally documented and procedures in place for the registration and deregistration of accounts. This includes provisioning unique user ID's for the employee. The registration process should be carried out for any information service that the user needs access to and should include regular audits to ensure user accounts are disabled when a staff member leaves their role. This control is primarily about authentication.

9.2.2. USER ACCESS PROVISIONING.

While the previous control described the authentication process staff should go through to log into an account to access a server, the level of access the user requires is described here. During the user provisioning process, specific rights and permissions will need to be granted to the employee and these rights should be recorded in a central repository which makes auditing and reviewing them easier. It can reasonably be expected that an employee may change roles one or more times during their time with your organization. During these role changes the level of access and rights the user requires can fluctuate and regular reviews can counter privilege creep; where long serving staff retain access to systems they no longer have a business need to access. With correct access management we can reduce risks and if we specify sanctions for any unauthorized access attempts a staff member might make we will improve our security posture.

9.2.3. MANAGEMENT OF PRIVILEGED ACCESS RIGHTS.

Privileged access should be strictly controlled as it allows the employee to circumvent security controls. A good example of this is not allowing staff to use root or admin accounts to perform their daily duties, and only using those privileged accounts when there is a specific need. The privileged access usage should be clearly documented including which users can access privileged rights and for which services. Requiring users to authenticate with their unique ID allows us the ability to audit the use of these accounts and to check and protect against abuse of privileged access. The access such be reserved and only used if there is an absolute need. There should also be a documented procedure outlining the authorization process required to gain access to this privilege level.

9.2.4. MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS.

One of the biggest risks that is often ignored at companies is how a user's credentials are provided to them, and managed. An example of poor practice is if a company's IT department simply emails passwords to users in clear text and with no requirement in place for the user to change their password or keep it secret. Proper password management should ensure credentials are sent to users over a secure medium in a co-ordinated and documented way, with steps taken to ensure that the user changes their password once received and acknowledges receiving it. The user should have to agree to a password policy that describes not only password requirements such as complexity but password management best practises such as not sharing it, or keeping it written on a post-it under your desk.

9.2.5. REVIEW OF USER'S ACCESS RIGHTS.

Users roles change over time. What access a user requires now, may not be what they require in 6 months' time. In many companies long serving employees can move between roles throughout their time with the organization. Having regular audits or reviews of user access rights can ensure that rights a user has retained from a previous role can be removed when no longer needed.

9.2.6. REMOVAL OF USERS OF ACCESS RIGHTS.

When an employee leaves the organization or their contract changes often the level of access the require for different services changes. In this case un-needed access should be removed then and there to prevent permission creep. This also extends to informing relevant staff of the role change to avoid un-intentional disclosure of information.

SECURITY CATEGORY – 9.3. USER RESPONSIBILITIES

9.3.1. USE OF SECRET AUTHENTICATION INFORMATION

As discussed with Control – 9.2.4 all staff should be made aware that they are responsible for their account, credentials and the use, or misuse, of the same. Staff should not share their passwords, have them stored in an unsecure form (post-its!), reuse the same password where SSO isn't in use and should adhere to the organizations password guidelines (min length, use of passphrases etc).

SECURITY CATEGORY – 9.4. SYSTEM AND APPLICATION ACCESS CONTROL

9.4.1. INFORMATION ACCESS RESTRICTION.

As discussed in previous controls access to information should be decided based on the employee's clearance level (are they authorized to view this information?) and their business need (do they need access to this data to do their job?). For this we need to define what the employee can do with the information (read, write, delete), their rights to access the application and even restricting what the user sees in their view to only what they have access to.

9.4.2. SECURE LOG-ON PROCEDURES.

The access to systems should be controlled with login procedures, such as secure login portals. This requires us to have clearly defined log-on processes and procedures that are easy to understand and use. They should not give information about the type of system being accessed, as this could aid an attacker in exploiting a service if they know the version for example, and it should be secured against unauthorized access.

9.4.3. PASSWORD MANAGEMENT SYSTEM.

The importance of password management cannot be overstated. Having an interactive password management system that forces users to log in, provides them with the capability to change their password and enforces your company's password policy. This then provides applications that the user wishes to log into with a hash, key, ticket or similar without the application ever needing to have access to the user's clear text password. This not only encourages good password practises for the user, but it also limits what systems house a user's password reducing the impact of a system being compromised.

9.4.4. USE OF PRIVILEGED UTILITY PROGRAMS.

When an application on our home pc crashes many times we simply open task manager(ctrl-alt-del) and close that application. We can do this even for applications run by other users on the computer and for applications and tasks used to keep the operating system running. As you can imagine this opens the risk of causing system instability. Other utilities can allow us to alter the integrity of data or even override access controls among other, damaging actions. While they are useful for resolving some problems the use of these tools should be heavily restricted to prevent abuse. Audit trails should be maintained for the use of these and users should be required to authenticate.

9.4.5. ACCESS TO PROGRAM SOURCE CODE.

Source code for any application should be protected as much as possible. There are many reasons for this but two good examples are; If a person has access to source code they can review it for potential exploitability or, for integrity, if we rely on tools for certain server operations when doing forensic investigating to find the cause and extent of a potential breach, we must be certain that those tools haven't been tampered with, are accurate and are performing as intended. Changes to code, including for patching/updates should be done in a controlled and documented manner. This should include having a back out strategy and maintaining a log of any changes.

SECURITY CATEGORY – 10.1. CRYPTOGRAPHIC CONTROLS

10.1.1. POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS.

Cryptography is a great way to ensure confidentiality that all companies can make use of. With the industry standard symmetric encryption being the free to use AES standard that can be used by any organization to encrypt all its data, effectively locking it to prevent unauthorised people reading its contents. By using a single key to lock and unlock that data it can play an essential role for any organization that deals with PII or other sensitive data. A more complex encryption type can be found in asymmetric encryption, such as RSA which uses one key to encrypt and another to decrypt and provides the additional functionality of non-repudiation and integrity checks.

As you can see encryption should play a major role in your security posture and your documentation should require its use if you deal with data you need to keep private. Any security policy you write that deals with the storage or transmission of data should have the use of encryption worked into it and described I procedural documents.

A good summary of encryption can be found in the Security+ training videos by Professor Messer found here;

https://youtu.be/W5su65wwd0g

https://youtu.be/z2aueocJE8Q

10.1.2. KEY MANAGEMENT.

If you decide to use symmetric or asymmetric encryption then key management plays a large part in how secure you are. With Symmetric encryption, you have a single key that needs to be distributed to anybody who has a legitimate need to decrypt and view data. For asymmetric encryption, we only must worry about one of the two keys, the private key. The other, our public key, should be managed in a way that ensures anybody can access it. In all cases we need to have policies in place outlining the entire lifecycle of the keys, from the creation, distribution, use, storage and disposal.

Also, important to note when creating your policies is if you will use some form of key escrow, where we store the keys we should keep safe with a third party as a safeguard. This can allow your keys to be accessed in certain circumstances such as if a court order is issued.

SECURITY CATEGORY – 11.1. PHYSICAL AND ENVIRONMENTAL SECURITY

11.1.1. PHYSICAL SECURITY PERIMETER.

Security concerns the physical domain as well as digital. Data, whether it is stored in paper or electronic form needs to be protected and the physical security of your organization should play a factor in your security planning. This can be looked at on various levels, such as not having your office in high risk environments like a high crime area, a hurricane prone region or like more grounded concerns like not having your datacentre and server rooms on the ground floor just off reception. Security guards, badges, door locks, filing cabinets and more all can come into play in a good, multi-layered security environment and an assessment of secure your physical perimeter is always a good starting point.

11.1.2. PHYSICAL ENTRY CONTROLS.

Having access controls within your office environment to prevent unauthorised persons from entering is very important. Nobody should be able to just walk in off the street and into your server room. Visitor sign-in should be required for anyone visiting. Providing your staff with physical ID badges and requiring them to keep the badges visible when in the office will allow unauthorized persons to be more quickly identified. More advanced physical controls can include multifactor authentication door locks that are restricted to certain individuals, identified by biometrics and their RFID ID card; or even turnstiles and man traps to better control the flow of people through key areas.

11.1.3. SECURING OFFICES, ROOMS AND FACILITIES

Depending on what is being protected we can better protect our valuable data. Not identifying individual offices with signs designating their purpose like “printing room”, ensuring the more important data processing offices in our organization are protected and behind several layers of physical security controls such as doors, ID checks and similar. While leaving less important processing rooms closer to public areas we can better protect our sensitive data from unauthorized access. Other concerns for rooms would be ensuring the walls segment the floor and ceiling crawl spaces.

11.1.4. PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL

As discussed part of good physical security practice flows into deciding where to place your office, avoiding areas that suffer from natural disasters can be a good way to avoid risks that could potential cost your company disruptions in availability and resources should a disaster occur. It is important to ensure there are adequate CCTV, Motion Detectors, Smoke/flame/heat detectors and other controls in place. While these and other technologies can form a great help one often overlooked requirement that can prove vital during physical incidents is ensuring staff are aware of what to do during an emergency.

11.1.5. WORKING IN SECURE AREAS.

Areas of your building where sensitive data is stored should have additional requirements and procedures for access. Areas should be locked when not in use with periodic monitoring. Secure areas should be treated in a similar way to data classification with access to and knowledge of the areas restricted on a security clearance and need to know basis. Having people work in teams and banning the use of person photo and video recording devices can both act to prevent misuse of the access granted to staff.

11.1.6. DELIVERY AND LOADING AREAS.

Many of the ways to implement this control have already been discussed such as mantraps, turnstiles, CCTV, guards, visitor sign ins and doors requiring authentication to open can protect areas that would traditionally have outside persons present, such as delivery drivers. Implementing these, and similar, controls limit the risk of intruders gaining greater access to your premise than required. Controls that are more specific to loading areas can include checking the incoming packages for unlawful or dangerous material, keeping records of what is brought in and shipped out and segmenting the delivery area by inbound and outbound shipping.

SECURITY CATEGORY – 11.2. EQUIPMENT

11.2.1. EQUIPMENT SITTING AND PROTECTION.

Don't leave physical equipment accessible to the public or in environmentally unsuitable areas. Work equipment, where possible, should be placed and used in secure areas where they can be access by authorized individuals to perform their required tasks. This can include environmental controls such as having a HVAC system in the data centre to keep temperature and humidity at an acceptable level, and including in your company policies restrictions on physical risks present by the employee, such as storing a glass of water on top of their desktop unit.

11.2.2. SUPPORTING UTILITIES.

For this control, its recommended to have redundancy for all our utilities (Telecoms, electricity, water, heating etc). For example, having multiple fiber connections with 2 or more telecoms providers gives us greater redundancy if 1 provider is suffering an outage, having a different type of telecoms connection such as satellite can provide even more redundancy. Applying the same thought pattern to other utilities can grant us greater uptime (such as using UPS' and generators for redundant power/electricity requirements). Monitoring for all utilities should be in place to give immediate notice of when there is a problem with any of these most basic services.

11.2.3. CABLING SECURITY.

The crux here is to avoid having cables easily accessible, within reach of people that are unauthorized to access the data being carried. Specialist cabling cabinets should be used when running cables through a building or, if possible, cables should be run underground. On a related note, to protect the integrity of the information being sent on data cables proper shielding should be put in place and the data cables should be kept separate from power cables.

11.2.4. EQUIPMENT MAINTENANCE.

Keeping devices and equipment in a good state of repair should always be considered best practice to prevent unexpected failures and malfunction. Schedule regular inspections of your equipment with staff who have the required skills to assess and maintain the relevant equipment. If using outside vendors to provide support ensure that for any equipment they and inspecting any data they should not have access to has been removed prior to their visit. If that is not possible the vendor should be vetted and screened to a level appropriate to the data being carried.

11.2.5. REMOVAL OF ASSETS.

Whenever we move an item outside of the organization we lose many of the controls in place to protect it. As such an authorization procedure should be in place that designate responsibility and requirements make sure

risks of removal facing those items are mitigated. This can include having a sign out procedure, giving time limits for equipment being moved off site and having handling guidelines. Authorization should always be required when equipment is moved off-site.

11.2.6. SECURITY OF EQUIPMENT AND ASSETS OFF PREMISES.

Part of taking assets off site should include maintaining a chain of custody for when the equipment changes hands. Records on who is in control of that asset at which time should be kept up to date. Other steps can include not viewing sensitive data in public, not leaving the asset unsupervised in a public place and taking reasonable steps to protect it from physical damage. Encryption should also be used for assets taken off-site even if encryption is not normally used in your organization. A higher standard of security should be given, where possible, to these assets.

11.2.7. SECURE DISPOSAL OR RE-USE OF EQUIPMENT.

A big security risk is the lack or a proper sanitation procedure for media at the end of its life. All media that holds non-public data should be zeroed before disposal. The higher the data classification of the media the more through the destruction of data. For the most sensitive data the media should be physically destroyed or degaussed. Deleting files or formatting is not enough for this type of data (this PII) as reusing, or allowing the reuse of the media could cause disclosure. Staff should be trained to follow the correct procedure for the safe disposal of media and instructions should be clearly documented. Another good practise for reusing old media is to never reuse media for lower classification purposes, for example do not reuse a top secret hard drive for a confidential or secret server.

11.2.8. UNATTENDED USER EQUIPMENT.

Users should never leave equipment unattended but if they do there should be controls in place to mitigate the risk. Technical controls can be a great help here such as having a screensaver timeout if a workstation is inactive for more than 15 minutes and requiring the user to enter their login credentials when they return to unlock it. This can prevent an unauthorized person accessing an employee's workstation and information if that employee leaves his desk without signing out. In Ireland especially, this can be a big risk as staff need to leave their desk to ensure their cup of tea is continuously full.

11.2.9. CLEAR DESK AND CLEAR SCREEN POLICY.

One of the easiest ways to find information in your office is to walk around, look at what post-its are on your staff's computer monitors, what documents have been left on their desks or are waiting to be collected in the printer. Requiring your staff to maintain a clean desk can prevent information from being accidently disclosed to staff that do not have clearance to view it, such as cleaners, or visitors temporarily in the office. Like the previous control the user should also be required to log off their workstation when leaving their desk and to be conscious of what is displayed on their screen and who is around them.

SECURITY CATEGORY – 12.1. OPERATIONAL PROCEDURES AND RESPONSIBILITIES

12.1.1. DOCUMENTED OPERATING PROCEDURES.

It is often best practice in IT to make sure you have all your systems and tasks documented. This is good for a few reasons; so, you don't forget how your systems are set up, to allow for knowledge of tasks and systems to be passed on to all your employees and to ensure, if something goes wrong there is sufficient information to remediate the issues in a timely fashion. The ISO standard follows a similar line of thought and recommends we document any task that involves information processing. These tasks can include installation, initial configuration, backups, scheduling restrictions, commonly encountered errors, how issues can be escalated and how information should properly be handled.

12.1.2. CHANGE MANAGEMENT.

Change management should always be comprehensively and clearly documented and with defined steps. At the very least this documentation should outline an approval process where the requested changes are submitted to, an assessment of the risks associated with the plan, mitigating steps to limit the risks, an agreement/approval stage, a testing phase once the technology has been deployed and a rollback plan if things go wrong. This is INFRASTRUCTURE focused, changes to the network and servers applications run on.

12.1.3. CAPACITY MANAGEMENT.

If our resource use exceeds our capacity we can suffer a loss of availability of that service. We should always balance these and plan ahead to ensure we always have sufficient capacity for our operations. This can be capacity planning for internet bandwidth in your office, so staff can carry out their day to day tasks, as well as redundancy in capacity for IT systems, so services are able to meet the needs of all their users. This stage is important and has spun off its own category of systems administrators who specialize in IT capacity management. These staff ensure there is always sufficient capacity on your information systems to avoid legitimate requests being lost, or rejected. The onset of cloud architectures has reduced the complexity and expense of modern capacity management. All steps and safeguards we have in relation to capacity management should be documented.

12.1.4. SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS.

Many organizations implement some form of change management. The most basic involves deploying new code to a testing, or development, environment before putting that code on production servers. ISO recommends we have at least 3 separate environments to avoid the chaos and disruption of deploying untested code to live servers. Developers should be able to continually deploy code on their development environment before allowing QA/testers to check the code in a staging, or test, environment. Once changes are agreed as per the change management process then this code can be deployed to a production, or operational, environment, which is the environment the end users interact with. It is good practise to document each of the environment, keep them logically separate and have procedures in place for moving code between, and accessing, each one.

SECURITY CATEGORY – 12.2. PROTECTION FROM MALWARE

12.2.1. CONTROLS AGAINST MALWARE.

All companies run the risk of being compromised by malicious software and part of any company's security plan should involve having some form of antivirus to detect and contain any infections. In addition to this, users should be given awareness training to be able to identify outbreaks and to guard against some attack vectors, such as suspicious email attachments. A tiered approach should be taken with a baseline of protection and training given for all computers and then addition protections provided to assets housing or processing sensitive data.

SECURITY CATEGORY – 12.3. BACKUP

12.3.1. INFORMATION BACKUP.

No matter how secure we are, risk can never be completely eliminated and we should prepare for the day when we need to recover from an incident that has separated us from our valuable data. This can be in the form of lost information or lost configuration, having a strong backup policy protects us in these situation. By having important data regularly backed up, with those backups tested to ensure we can restore from them, we can limit the impact of an attack. When designing a backup policy, it is important to ensure that storage requirements and the value of the data stored is considered during planning. Best practices include keeping separate copies of the backups in geographically separate locations, minimizing time between backups to the company's acceptance of how much data can be lost and ensure staff are trained to be able to restore data from backups when required.

SECURITY CATEGORY – 12.4. LOGGING AND MONITORING

12.4.1. EVENT LOGGING.

On any system that processes information we should ensure we have auditing and logging in place, that cannot be tampered with by the users of that system. One way to accomplish this goal is to use rsyslog to store logs on a Linux or Unix machine remotely, away from the tampering of the local system. This control is important for any event that requires investigating and can help us find the cause of problems quickly and accurately. The level of logging should also be tailored to what is useful and what is useful depends on the type of information and purpose of this server. Too high of a logging level will lead to important log entries being overlooked due to the “noise” of excessive logging or even the servers hard disk filling up causing a crash or for older log entries to be overwritten. Too low of a logging level can lead to important event information not being recorded. Reviews of logs should be regularly carried out and logs should be kept according the retention period decided by what your organization deems necessary for investigations.

12.4.2. PROTECTION OF LOG INFORMATION.

Logs are only as useful as they are accurate. Steps should be taken to ensure users cannot alter log entries, either maliciously or accidently. Enough storage space should be available to reduce the risk of excessive log files being generated to overwrite previous, important, entries. In addition, only authorized staff should be able to view logs. Ways to ensure logs have not been tampered with include storing logs remotely using tools such as rsyslog and ensuring integrity is maintained using file hashes.

12.4.3. ADMINISTRATOR AND OPERATOR LOGS.

Who watches the watcher? The age-old question can give security teams sleepless nights. The system owners, administrators, often have root or administrator privileges. To protect against abuse any use of these privileges should be recorded and reviewed. Likewise, the audit trail kept should be stored in a way that the administrator cannot tamper with.

12.4.4. CLOCK SYNCHRONIZATION.

As important as logs are they can simply add to the confusion if an organizations logs don’t follow a standardized data/time format and time zone throughout the various time zones the company operates in. While this may not be an issue for organizations based in the one time zone best practice dictates the organization decides on a time zone and format to follow and enforces that on all its assets and logs. This is known as your reference time. In many cases organizations settle on UTC for their reference time.

SECURITY CATEGORY – 12.5. CONTROL OF OPERATIONAL SOFTWARE

12.5.1. INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS.

Installing, or allowing the installation of unknown or untested software can introduce system instability, malware and other risk. Any new software installations should need to follow a standard procedure to be approved and installed. This installation should be carried out by the organizations IT team, untrained staff should never be able to perform this function and the team performing installations should first test the new software for compatibilities issues, vulnerabilities or similar.

SECURITY CATEGORY – 12.6. TECHNICAL VULNERABILITY MANAGEMENT

12.6.1. MANAGEMENT OF TECHNICAL VULNERABILITIES.

Having a vulnerability management program in place can be very important for learning about individual vulnerabilities and the risks surrounding them. This proactive measure can allow your team to more quickly respond to new threats and put in place mitigating steps to reduce the risk of them if remediation is not immediately possible. Using vulnerability scanners for this can be an important step towards comprehensive coverage and with tools such as Nessus, Nexpose and Qualys, among others, organizations have many tools to choose from.

12.6.2. RESTRICTIONS ON SOFTWARE INSTALLATION.

Similar to requiring trained staff for software installations there should be rules and restrictions in place on what software can be requested, used and installed. Restrictions should be in place to ensure staff can only have software they need to do their job installed and this should cover all levels of the organization. This will drastically reduce the risk of malware being introduced to your environment. There are two ways to go about this, blacklisting software explicitly states what software is not allowed to be installed in your environment and can be used to prevent known trojan horse application and spyware from being installed. Whitelisting software explicitly states what software can be installed and is a more restrictive option, with whitelisting only software that has been specifically tested and approved can be used.

SECURITY CATEGORY – 12.7. INFORMATION SYSTEMS AUDIT CONSIDERATIONS

12.7.1. INFORMATION SYSTEMS AUDIT CONSIDERATIONS.

Any investigation and audit of information systems should be planned and coverage agreed on. The audit should not change any information being reviewed and the auditors access should be monitored and logged. Ideally the auditor should have read only access and should only run their audit scripts outside of business hours to minimize disruption.

SECURITY CATEGORY – 13.1. NETWORK SECURITY MANAGEMENT

13.1.1. NETWORK CONTROLS.

Your network is how your staff and users access your information systems. That same network, if not adequately protected can allow a malicious user to try and compromise your environment, or if an asset is already compromised to more easily move around. There are many ways to protect your network and the level of protection should depend on your environment. Access should be restricted and controlled to protect against misuse and abuse. ISO 27033 discusses network security in detailed and should be reviewed in relation to this control category.

13.1.2. SECURITY OF NETWORK SERVICES

In addition to segmenting you network you should include additional controls such as firewalls to control access, NAC's and filtering to restrict access to approved users/devices and NIDS and NIPS to monitor for abuse. Other tools can be used and should any service contracts your company enters into should include requirements for protection levels.

13.1.3. SEGREGATION IN NETWORKS.

Your network should be divided into subsections based on the users, application type and classification of data held in that environment. There are many ways the segment the network such as using VLANs or firewalls and time should be spent to plan out this segregation to ensure optimal protection and separation.

SECURITY CATEGORY – 13.2. INFORMATION TRANSFER

13.2.1. INFORMATION TRANSFER POLICIES AND PROCEDURES.

The process that employees need to follow should be explicitly stated including an acceptable use policy which employee's need to sign to transmit information. These policies should include measures to prevent staff from forwarding malicious mail, engaging in harassment and should detail the retention period and disposal procedure for emails, when encryption should be used and steps to protect against information disclosure such as being overheard having confidential conversations in public places.

13.2.2. AGREEMENTS ON INFORMATION TRANSFER.

Where feasible during communications with vendors, government and other parties it should be explicitly required in agreed contracts what level of security is required for correspondence. This should keep include non-repudiation, responsibilities in the event of disclosure, technical requirements and data classification.

13.2.3. ELECTRONIC MESSAGING.

As more and more companies use Electronic Messaging, such as email, Lync and Slack, in their day to day communications repertoire and sometimes exclusively it is important that we have policies in place detailing how email can be used and what controls are in place to protect us such as keeping a record of messages exchanged, encryption and non-repudiation.

13.2.4. CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS.

Staff, contractors and other third parties working in your organization may all have access to confidential information. This needs to be protected and one of the best ways to do this is to require all parties with access to sign confidentiality or non-disclosure agreements(NDA). These agreements should specify what is to be kept confidential, for how long, what the penalties are for disclosure, what the protected information can be used for and how that information should be protected and disclosures reported.

SECURITY CATEGORY – 14.1. SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

14.1.1. INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION.

Security should be an integral part of the development and acquisition of all new information systems. This means including any security needs as deliverables/requirements at the earliest possible point in development or acquisition. The tenet of "If it doesn't work securely, it doesn't work."[1] should apply when planning, developing, testing and deploying applications. The level of security should be a reflection of the value of the information being processed by the new application and its business criticality.

14.1.2. SECURING APPLICATION SERVICES ON PUBLIC NETWORKS.

Whenever our information processing takes place across public networks, such as the internet, we need to take steps to ensure the data isn't disclosed or modified and to ensure there is a level of non-repudiation. Using encryption such as transporting the data over a VPN, SSL/TLS or IPSec can provide us with protection against disclosures and making use of encrypted hashes (known as digital signatures) can provide us with a level of assurance that the information has not been modified. In a PKI setup, we can also achieve non-repudiation through the use of public-private key pairs.

14.1.3. PROTECTING APPLICATION SERVICE TRANSACTIONS

Special consideration should be given to information involved in transactions where data is modified on the service. Clearly defined procedures, database locking and other methods should be used to mitigate against this threat.

[1] Kelly Henderhan

SECURITY CATEGORY – 14.2. SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

14.2.1. SECURE DEVELOPMENT POLICY.

A policy should outline the security requirements required during information systems development. It should include controls to protect the development environment, guidelines on how to create secure code and testing the code to verify it is secure. There are many programming methodologies that can be incorporated into this control such as the Secure Software Development Lifecycle.

14.2.2. SYSTEM CHANGE CONTROL PROCEDURES.

This control ties into having a change management process and requires a similar process for deploying code during the development stage of new applications. It should include a risk analyse of impact, a roll back plan, testing and approval requirements. Documentation should be updated to accommodate changes and a version control record and audit log maintained. This is SOFTWARE FOCUSED.

14.2.3. TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES.

Change always makes information systems more vulnerable. Therefore, we have a test environment but even with that whenever we make changes to applications, we should run through application use cases and conduct tests to ensure the change hasn't negatively impacted usability or functionality.

14.2.4. RESTRICTIONS TO CHANGES TO SOFTWARE PACKAGES

Where possible we should avoid making changes to software packages. Changes can introduce new vulnerabilities, break functionality and may prove a resource intensive exercise. In some circumstances it is justifiable to take this risk for a business need. In these cases, we should make sure we have the vendors written consent to changes, document if the vendor will still support the software and make sure we run comprehensive vulnerability tests to help us assess the risk. It is also best practise to maintain a version repository of any changes made, including keeping a copy of the original.

14.2.5. SECURE SYSTEM ENGINEERING PRINCIPLES.

Principles, such as those described in NIST SP 800-160 should be formally implemented into the organizations methodology and process, documented and maintained to allow for secure software engineering throughout the software development lifecycle. These principles should also be reviewed annually to ensure they still represent current best practises.

14.2.6. SECURE DEVELOPMENT ENVIRONMENT.

The people, technology and development process should all be protected with consideration given to the classification of data to be processed, the business criticality, legal requirements, access control and backup requirements.

14.2.7. OUTSOURCED DEVELOPMENT.

With globalization resulting in more and more companies entering into partnership with outsourcing firms for their software development it becomes ever more important that the organizations security requirements are adhered to by their outsourcing partner. To ensure this is the case the company should actively work with and monitor the outsourced team to ensure compliance. Agreements should be in place to ensure the acceptance testing requirements are in place to include security concerns and that periodic auditing of the partners environment allowed.

14.2.8. SYSTEM SECURITY TESTING.

As security should be a concern at every stage of the project security testing should be conducted throughout development with the extent of testing dependent on the business criticality of the application.

14.2.9. SYSTEM ACCEPTANCE TESTING.

As previously stated “If it doesn’t work securely, it doesn’t work”. There should be clearly documented acceptance criteria for new applications, upgrades and patches that must be met before these changes are accepted and rolled out. These criteria should include security concerns and after testing any issues should be remediated.

SECURITY CATEGORY – 14.3. TEST DATA

14.3.1. PROTECTION OF TEST DATA.

Any data used for testing purposes should be taken from a carefully selected sample pool and given adequate protection. Avoiding the use of PII and sensitive data can help reduce the risks of disclosure. Standard best practices include mimicking the access controls for production environment on the testing environment, having a procedure for gaining authorization to use production data, maintaining an audit trail and ensuring the destruction of data when no longer needed.

SECURITY CATEGORY – 15.1. INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS

INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS.

Rules should be in place that govern what a vendor can access and how they should access it, as well as specifying other security requirements. These should require the security a vendor should have on their own network, how incidents should be reported and any other requirements your organization deems necessary, depending on the value of what the vendor will have access to. Having a policy outlining what is expected can help guide us when we are considering vendor relationships.

15.1.2. ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS.

The rules we set out in our Information Security Policy for Supplier Agreements should be included in all contracts with vendors and they should commit to upholding these requirements. Periodic auditing can be considered to ensure compliance.

15.1.3. INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN.

It stands to reason that if there is access allowed between your network and your vendors network, then any party with access to your vendors network potentially has access to your organization, such as your vendors suppliers. There should be policies in place to ensure access between you and your vendor is restricted and controls to protect against unauthorized access. Ensuring your organization and your vendor keep an audit and log trail to track access and requests can provide accountability and requiring your vendor to screen their suppliers can also reduce this risk.

SECURITY CATEGORY – 15.2. SUPPLIER SERVICE DELIVERY MANAGEMENT

15.2.1. MONITORING AND REVIEW OF SUPPLIER SERVICES.

This will provide us with the confidence that are suppliers are adhering to the security requirements of their contract. Reviewing the audit trail of a vendor, conducting vulnerability assessments on their network and engaging in regular meetings to ensure the vendor understands their obligations can all prove helpful.

15.2.2. MANAGING CHANGES TO SUPPLIER SERVICES.

Vendors should not be able to make any ad-hoc changes to their service. This can include patching, upgrades and improvements. Any changes should be managed to limit disruption and ensure service continuity in the event of problems occurring. This also gives us a chance to review our security posture and introduce new controls as required to ensure the changes do not weaken our security position.

SECURITY CATEGORY – 16.1. MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

16.1.1. RESPONSIBILITIES AND PROCEDURES.

Any security incident that could take place should have procedures in place to instruct staff how to act with responsibilities and roles clearly defined. This should cover all phase of an attack[2];

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Actions at all stages should have procedures in place, actions taken at each step should be logged and reviewed and, where necessary it should be possible to escalate incidents. When creating procedures creating a list of potential incidents should be considered.

16.1.2. REPORTING INFORMATION SECURITY EVENTS.

Your organization should document what constitutes a security event and the should have a single point of contact the should receive reports of these incidents. This point of contact can be a person but is more likely an Incident Response team. All staff should know who to contact in the event of an incident and should have a standardized process to lodge reports.

16.1.3. REPORTING INFORMATION SECURITY WEAKNESSES.

Giving staff training to help them identify security weaknesses, and having an easy to use reporting process to report their finding can greatly assist your security team with identify problems. Part of this training should discourage employees from trying to test or exploit the weakness they have found as this should be done by specially trained personnel only.

16.1.4. ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS.

An information security event indicates that the security of an information system, service, or network may have been breached or compromised. It indicates that an information security policy may have been violated or a safeguard may have failed. An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.[3] Trying to decide if an event constitutes an incident is an important

[2] http://blog.securitymetrics.com/2017/03/6-phases-incident-response-plan.html
[3] http://www.praxiom.com/iso-27001-definitions.htm

function of the point of contact but they may not work in isolation and the responsibility my fall on a dedicated Information Security Incident Response Team.

16.1.5. RESPONSE TO INFORMATION SECURITY INCIDENTS.

The intent behind the response is to prevent further compromising of the environment by containing the attacker. While the most obvious way of doing this can be shutting down the impacted servers it should be noted that in doing that we lose evidence stored on the machines RAM. Evidence collection should go hand in hand with the initial response and the assets affected should have an image of their hard drive taken and hashed and a chain of custody kept of who handles the original asset's data. Any testing or investigations should be done on copied images, never the original. Documented procedures should guide your team on how to correctly respond, who is to be notified and how evidence is to be collected and what the escalation process is.

16.1.6. LEARNING FROM INFORMATION SECURITY INCIDENTS.

The documentation on the incident that the organization has accrued and the experience its incident response team has gained should be used to digest how the incident was responded to with the intent on finding ways to improve the process. This can help us speed up incident resolution in future, or avoid them completely. In some cases, past incidents can be used for training new incident response staff and for improving organizational awareness.

16.1.7. COLLECTION OF EVIDENCE.

Evidence collection is vital if your organization plans to pursue charges and having specialist staff with training on how to properly collect evidence and store it is vital to ensuring the evidence can be admitted to court. ISO/IEC 27037 goes into detail on evidence collection and should be read and documented procedures written. Staff should then receive training on those procedures and only those trained staff should be involved with evidence collection.

SECURITY CATEGORY – 17.1. INFORMATION SECURITY CONTINUITY

17.1.1. PLANNING INFORMATION SECURITY CONTINUITY.

Having comprehensive business continuity and disaster recovery plans can be vital for in organization's survival should a disaster occur. Such plans should be sure to include security which is still important, if not more so, during a crisis and should be included in any plans created. If there are no such plans then the organization should strive to maintain security at its normal level during a disaster. If possible Business Impact Analysis' should be carried out to investigate the security needs during different disasters.

17.1.2. IMPLEMENTING INFORMATION SECURITY CONTINUITY.

Ensuring that security controls in any plans are carried out in a disaster is just as important as having the plans themselves. There should be documented processes and procedures in place and easily accessible to staff during such a situation. These documents should be available in both electronic and paper format, with copies stored in geographically separate locations. This should allow us to maintain a command structure that includes security responsibilities, and keeps staff accountable and aware that security is still necessary. In some types of disasters our primary security controls may fail, in this case we should have separate, mitigating controls ready to be implemented.

17.1.3. VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY

This helps us ensure our plans are effective and will work as intended. In practice, it is carried out through table-top exercises, structured walkthroughs, simulation tests, parallel tests, and full interruption tests.[4] The plan should be updated to reflect changes in the organization, frequently tested to ensure it works as envisioned and that everyone involved is trained to know what to do with a disaster strikes.

[4] https://en.wikipedia.org/wiki/Disaster_recovery_plan#Testing_the_plan

SECURITY CATEGORY – 17.2. REDUNDANCIES

17.2.1. AVAILABILITY OF INFORMATION PROCESSING FACILITIES.

A key tenet of security is ensuring availability and this can be better enforced by using redundancy. This is simply having multiple redundant components so that if one fails operations fail-over to the remaining, working components. This can be expensive and what applications are in scope for this redundancy should be in line with the business needs.

SECURITY CATEGORY – 18.1. COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

18.1.1. IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL REQUIREMENTS.

All companies should adhere to their contractual and regulatory obligations, but to do so we need to know what those obligations are. Your organization should take care to go through its contracts and understand what is expected of you. You should also have specially trained staff with knowledge of regulations impacting your industry at hand when drafting policies, procedures or stands. These staff can keep you informed of changing requirements so you can be sure to include them to ensure you are compliant. Remember, if you have offices in multiple legal jurisdictions your plans should take the different legal environments into account.

18.1.2. INTELLECTUAL PROPERTY RIGHTS.

You should make sure that, for any material you use such as software, you are compliant with copyright and IP laws, as well as any licensing fees that may apply. Ensuring that software on your assets has been attained from the vendor, and that only correctly licensed versions can be installed we can reduce our risk. Outlining employee responsibilities, such as not using pirated software, in the Acceptable Use Policy can help us be compliant, as can regular audits of software. Be prepared to hand licensing information to the vendor should they wish to audit you.

18.1.3. PROTECTION OF RECORDS.

In many jurisdictions there is legislation in place to specify how record retention should be carried out. An example of this from the GDPR is for healthcare records[5];

> "In general, medical records should be retained by practices for as long as is deemed necessary to provide treatment for the individual concerned or for the meeting of medico-legal and other professional requirements. At the very least, it is recommended that individual patient medical records be retained for a minimum of eight years from the date of last contact or for any period prescribed by law. (In the case of children's records, the period of eight years begins from the time they reach the age of 18)."

You should have policies in place to protect records in accordance these laws, as well as contractual and regulatory requirements. Similarly, you may wish to tailor your retention policy in a manner that benefits your organization and helps further your business needs. This can be done but should be carried out in line with legislation, regulatory and contractual requirements. Keeping records for too long, beyond a reasonable need for the business can cost resource in maintaining them and we run the risk of greater loss should a breach occur, with that in mind it is encouraged to limit the retention period of records where reasonable.

18.1.4. PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION.

[5] https://www.icgp.ie/go/in_the_practice/it_faqs/managing_information/8E2ED4EE-19B9-E185-837C1729B105E4D9.html

Nearly all countries have some requirements for reasonable protection of collected PII. In some jurisdictions, such as the European Union and the incoming GDPR, not sufficiently protecting PII can cause fines to be leveraged against the organization. To use the GDPR as an example a company can be fined up to 4% of its annual revenue. One of the best ways to best ensure compliance is to designate an employee a Privacy Officer who can advise on local regulations.

18.1.5. REGULATION ON CRYPTOGRAPHIC CONTROLS.

In a previous control we discussed the importance of using encryption for confidentiality, integrity and non-repudiation, but in some states the use of encryption is heavily regulated, and in some cases, require decryption keys to be provided to the authorities. It is important to understand your local laws when using encryption or incorporating encryption in your products.

SECURITY CATEGORY – 18.2. INFORMATION SECURITY REVIEWS.

18.2.1. INDEPENDENT REVIEW OF INFORMATION SECURITY.

Internal auditors can be subject to undue influence or interference from their co-workers. The best way to gain an impartial and accurate view of your security landscape is to contract independent auditors to do a security audit. If internal auditors must be used they should have executive level authority. These reviews can help find gaps in your security or areas that can be improved. The auditor should provide a report to management with their findings and recommendations.

18.2.2. TECHNICAL COMPLIANCE REVIEW.

Having skilled staff run regular compliance and vulnerability scans can help you measure your environment and help direct remediation efforts. Penetration tests can also be considered. While more intensive and expensive penetration testing can find issues, automated scanners may miss and should not be overlooked. The process of compliance reviews should be documented to include approval, scope to be assessed and a summary of what is to be checked and the methodology used.

SUMMARY

As you can easily see ISO27001 really does cover every aspect of managing your information securely. From vendor relations and the hiring process to secure software development and infrastructure change management every aspect is touched on. Not all controls and control categories will be applicable to your environment but by tailoring these controls down to what is you are in an advantageous position to use these as a roadmap to improving your organizations security.

The entire purpose of this document was initially to act as a quick reference for myself to read back on in months or years' time but the scope of it evolved while I was writing it. The new scope is to act as a learning tool for people looking for a high-level discussion of the controls needed to become ISO27001 certified without going into the level of detail required for actually implementing them. If you want to implement ISO 27001 after reading this document it is advised that you look into the ISO27002 standard which gives detailed advise on obtaining compliance.

This will be a document I will revisit and update as I continue my journey.

REFERENCES

Gamma Secure Systems Limited. (n.d.). *The new versions of ISO/IEC 27001 and 27002 are now International Standards*. Retrieved from gammassl: http://www.gammassl.co.uk/27001/revision.php

Guha, S. (Director). (2014). *Transition to ISO IEC 27001:2013* [Motion Picture].

Handerhan, K. (n.d.). *ISC2 CISSP*. Retrieved from Cybrary: https://www.cybrary.it/course/cissp/

Kosutic, D. (n.d.). *ISO 27001 vs. ISO 27002*. Retrieved from advisera: https://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/

Lupa, C. V. (n.d.). *ISO/IEC 27001. Information Security Management System.* Retrieved from Udemy: https://www.udemy.com/isoiec-27001-information-security-management-system/learn/v4/overview

Rafiandi, A. (Director). (2015). *What is ISO 27001:2013* [Motion Picture].