ISMS Manual:
Designing, Implementing and Managing an ISMS

Executive Summary

Organisations should consider developing and implementing an Information Security Management System ("ISMS") to ensure that their "information assets" (data) are fully protected regarding the following three principles:

- ***Confidentiality*** (ensuring that their information assets are not disclosed to persons or systems that do not have the authority to access them)
- ***Integrity*** (ensuring that their information assets are not modified without proper authority, ensuring that they can be trusted to be true and accurate)
- ***Availability*** (ensuring that their information assets are available when they are needed)

Protecting information assets alone would not guarantee that these three principles can be maintained: there is also a requirement to understand the risks associated with their "supporting assets", upon which the security of information assets will depend (e.g. premises, hardware, software, networks, media and people).

An organisation's ISMS will provide a business risk approach to the design, implementation, operation, review, improvement and management of information security. This will involve:

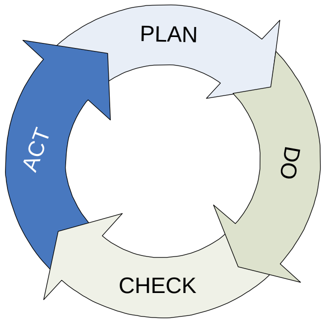
- The provision of effective information security policies, processes and procedures
- Developing an organisational structure and resources to support information security
- Providing thorough training to ensure personnel, contractor and third-party awareness
- Undertaking detailed risk assessment activities to identify, manage and remove risks
- Addressing and resolving information security incidents promptly
- Monitoring and improvement activities, including management reviews and internal audits

There are two important documents that need to be in the possession of organisations who are seeking external certification of their ISMS:

- ISO/IEC27001:2013 - the Management Systems Standard. This specifies the standard which is to be assessed, specifying the activities, documents and records that are required. This is the document that organisations seeking external certification will be assessed against by their external auditor.
- ISO/IEC27001:2013 – Annex A. This document contains key information on how to protect information assets and provides a list of controls (or good business practice) that helps in achieving this. Both information and supporting asset risk assessments use these controls extensively. This document is derived from and aligns with ISO/IEC 27002.

More specifically, these standards require the following approaches to be adopted:

- All information security activities shall be undertaken in accordance with agreed, published and current policies, processes and procedures, with records produced to support this.
- The organisation must establish, communicate and report progress against a number of information security objectives: what is the organisation trying to achieve from its ISMS?
- Information assets (and their supporting assets) should be identified and assessed against all relevant risks, which should be removed or reduced to an acceptable level where possible.
- The manner in which an organisation protects its information assets (and supporting assets) shall be by the effective implementation of controls (from ISO/IEC 27002, for example).
- The ISMS must be subject to regular auditing, monitoring and management review, and be subject to continual improvement:

PLAN Establishing the ISMS **DO** Implementing and operating the ISMS **CHECK** Monitoring and reviewing the ISMS **ACT** Maintaining and improving the ISMS	

1.0 Management Commitment

(ISO/IEC 27001:2013, Section 5.1)

For an ISMS to be established, it is essential that Executive Management within an organisation must make a commitment to all elements of the system, including its design, implementation, operation, monitoring and review and improvement activities. Further, they need to communicate this effectively to the employees, contractors and any third parties involved in delivering the ISMS, ensuring that they in turn have the appropriate levels of training, awareness and competency to deliver ISMS related tasks. Risk ownership resides at the very top of an organisation and should not be delegated.

Specific tasks required by Executive Management include:

- Defining the scope and boundaries of the ISMS – is this to be implemented for the entire organisation or just specific areas, functions or departments? (see **ISDL325**)
- Defining and communicating the organisation's ISMS Policy (see **ISDL01**).
- Establishing information security objectives and plans: the targets that the organisation aspires to achieve through the operation of an effective ISMS.
- Agreeing the roles and responsibilities necessary for the operation of the ISMS and ensuring that sufficient resources are made available for it to be operated successfully (see **ISDL10**).
- Promoting an effective programme of information security awareness, including communicating the importance of the Information Security Policy.
- Deciding upon the organisation's approach to risk management and risk treatment, including the frequency with which risk assessments are to be undertaken.

- Deciding upon the organisation's level of acceptable risk: an important decision that is carried into risk assessment activities, and that needs to be reviewed regularly.
- Participating in management reviews at planned intervals to understand the ongoing ISMS activities, levels of compliance, and whether objectives and plans are being achieved (see **ISDL09**).
- Ensuring information security within the organisation complies with all applicable legislation and contractual requirements, as a core element of corporate governance (see **ISDL390**).

2.0 Determining the Scope of the ISMS

(ISO/IEC 27001:2013, Section 4.3)

Once Executive Management have committed to establishing an ISMS, the next step is to understand to what extent it will apply to the organisation (see **ISDL325**). It may be considered appropriate or beneficial to include the whole organisation, or there may be specific divisions or departments to which information security specifically applies. Matters to consider:

- Are there advantages/disadvantages of including the whole organisation in scope?
- If the organisation is vast, has consideration been given to separate ISMS implementations?
- Are there only specific locations or activities that need to be included in the scope?
- Are there only specific technologies or client requirements that need to be in scope?
- Are there any laws, legislation or regulation that will affect what is included in scope?
- Are there any third parties or suppliers that need to be in scope?

3.0 Defining the ISMS Policy

(ISO/IEC 27001:2013, Section 5.2)

The Standard mandates a "top level" ISMS Policy, that should be tailored to reflect the specific nature of the organisation, its locations, operations and technologies. This Policy should clearly reflect:

- How the ISMS objectives and goals are established
- Any identified legislative, regulatory or contractual information security requirements
- How it aligns with the organisation's strategic approach to risk management
- How risks will be assessed and managed
- That it has been approved by management

It is also common for the ISMS Policy to refer to other Information Security related policies (e.g. Asset Management Policy, Acceptable Use Policy etc.).

4.0 Patch Management

(ISO/IEC 27001:2013, A.12.6.1)

The goal of patch management is to keep the assets that form part of the information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

Without regular vulnerability testing and patching, the information technology infrastructure could fall foul of problems which are fixed by regularly updating the software, firmware and drivers. Poor patching can allow viruses and spyware to infect the network and allow security weaknesses to be exploited.

4.1 Vulnerability Scanning and Penetration Testing

- All hardware and software will be scanned using a vulnerability scanner to identify weaknesses in the configuration of systems and to determine if any systems are missing important patches, or software such as anti-virus software.
- All product hardware and software will be scanned by a first party vulnerability scanner at least once per quarter.
- All product hardware and software will be scanned by a third-party vulnerability scanner at least once per year.

- All products will be tested by a third party, CREST certified, penetration tester at least once per year.

- The organisation's IT infrastructure will be scanned by a third party at least once per year.

- Remediation will be undertaken of any vulnerabilities identified.

4.2 Identifying Patches to be Applied

- The organisation's anti-virus server will be configured to automatically download the latest virus and spyware definitions and push them to the servers, PC's and tablets running on the network.

- Windows patch management tools will be utilised to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.

- Azure Update Management will be used to scan for compliance and apply software updates to machines in Azure and hybrid cloud.

- Security weaknesses and software update notifications issued by special interest groups will be monitored on a regular basis and any critical issues affecting the organisation's IT infrastructure will be acted upon immediately.

- Notifications of patches from cloud, application and database vendors will be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the supplier's website will be reviewed on a regular basis.

- All vulnerabilities identified in penetration tests or vulnerability scans will be added to the ISMS and categorised. Mitigation timeframes are fixed for each category:
  - *Critical* – No later than 2 weeks from identification (faster if configured for immediate rollout)
  - *High* – No later than 4 weeks from identification
  - *Medium* – No later than 6 months from identification
  - *Low* - No later than 12 months from identification

4.3 Types of Patches

The following patches will be implemented on the different information infrastructure types.

Type	Patch
Web Applications	Vulnerabilities, security updates
Server / Computer	BIOS, firmware, drivers
Operating System / Application Software	Service packs, patches, feature packs
Router and Switches	Firmware
Anti-Virus / Anti Spyware	Data file/Virus definition update

4.4 Roles and Responsibilities

The owners detailed below will be responsible for patch management.

Role	Owner	Comments
Patch identification	Infrastructure	Responsible for identifying patches for the application systems which they own or administer.
Technical Patch Administration	Infrastructure, IT Support	Responsible for patch approval and ownership of all technical updates, including: • Operating systems • Patches for PC's and servers • Antivirus and antispyware • Firmware • Printer drivers
Technical Release Administration	Product Managers, IT Support	Responsible for the planning, building, testing and deploying new software.
Application Patch Administration	Infrastructure, DevOps	Responsible for patch approval and ownership of all application updates.
Vulnerability & Security scanning	Infrastructure, Information Security Manager	Responsible for scanning the components on the network for security weaknesses and missing patches.

4.5 Patching Schedule

The product's **hardware and software** will be patched according to this schedule:

Time	Action
Daily	• Anti-virus and spyware definitions will be configured to be installed automatically as they are released.
Weekly	• Critical security patches reviewed and approved as required.
Monthly	• Public facing servers – apply all outstanding patches.
Quarterly	Apply all outstanding patches. • Check that drivers are up to date. • Review vulnerability scans and remediate as required.

The organisation's **IT infrastructure** will be patched according to this schedule.

Time	Action
Daily	• Anti-virus and spyware definitions configured to be installed automatically as they are released
Weekly	• New software releases reviewed and approved as required • Microsoft critical updates, and security updates configured to be approved for rollout as they are released
Quarterly	• Check that drivers are up to date • Check for BIOS updates
Six monthly	• Review vulnerability scans and remediate as required

5.0 Bounty Management

All emails from ethical hackers should be forwarded to infosec@accessintelligence.com for review. We do not engage in conversation to bounty emails.

The Information Security Manager will review the legitimacy of the vulnerability and record it in the ISMS, if necessary. Access Intelligence will only respond if this review shows the vulnerability to be of a serious nature by a serious actor. Only in these exceptional circumstances, a bounty may be paid after Executive Management approval.

6.0 Establishing a Risk Assessment Methodology

(ISO/IEC 27001:2013, Section 6.1.2)

The Standard simply requires that an organisation identifies a risk assessment methodology that is suited to the ISMS, and any identified business information security, legal and regulatory requirements. It does not provide any detail on how the methodology should work, so this section covers the elements that should be incorporated into an effective approach.

An organisation needs to establish an effective risk assessment methodology for identifying threats and vulnerabilities that may affect the confidentiality, integrity or availability of its information assets. This will also require the methodology to be applied to the supporting assets upon which the security of information assets depends.

Both information assets and their supporting assets are subject to a wide variety of threats, each of which has the potential to exploit a vulnerability and produce an event that damages or disrupts the normal, secure existence or operation of the asset. Threats can originate from inside an organisation as well as external sources and may be the result of accidental or deliberate events. A vulnerability alone cannot harm an asset: rather it is a condition or state that could allow a threat to exploit it and consequently cause harm. Therefore, threats and vulnerabilities need to combine to create an incident that can damage or disrupt the normal, secure existence or operation of the asset.

Whilst the ISO27001 standard does not specify one specific risk assessment methodology that should be used, an approach should be based upon a methodology that includes the following activities:

- Evaluate the risks which have the potential to affect the confidentiality, integrity or availability of the asset being assessed
- Identify the individuals who are responsible for the risks ("risk owners")
- Understand which controls have already been selected and implemented in order to protect the asset from the risk
- Against the knowledge of existing controls, assess the probability and impact levels if the risk were to happen
- Compare this result against the organisation's acceptable level or risk (already defined by Executive Management in Section 1)
- If the risk level is higher than that which is acceptable to the organisation, implement a risk treatment activity (see Section 6)

7.0 Establishing a Risk Treatment Methodology

(ISO/IEC 27001:2013, Section 6.1.3)

Once a risk has been identified as being higher than the organisation's acceptable risk level, a number of options are available for how to address this situation. The decision as to which risk treatment option to pursue needs to be made by the organisation, considering factors such as:

- the likely frequency of the risk happening
- the costs and impacts of each risk occurrence (in terms of business disruption, labour budgets, financial penalties, contractual issues etc.)
- the availability of alternative or improved controls, and the resources to implement them
- the organisation's approach to accepting known risks

7.1 Reducing the Risk

The most common approach to treating identified risks is to review and change the way in which existing controls operate. By selecting new controls, or the improved management or operation of existing controls, it should be possible to either (a) reduce the likelihood of the underlying vulnerability from being exploited or (b) reducing the impact by being prepared for the risk and how to react to it.

All controls from Annex A of ISO27001 can be implemented with varying degrees of effectiveness, and there is often room for improvement. Additional controls should be selected based upon their relative strengths, and whether their foundation is in prevention, detection, monitoring, training etc.

7.2 Accepting the Risk

There are some circumstances where an organisation cannot implement effective controls to prevent a risk, or the financial cost of implementing improved controls is prohibitive and may exceed the value of the loss or disruption to the organisation. Should this be the case, then all stakeholders need to be consulted and confirm their agreement to the reasons why the risk is to be accepted, before the risk acceptance is signed off. If the stakeholders cannot agree to accept the risk, but the costs associated with changing controls are too high, the option of transferring the risk (Section 6.3) should be pursued.

Once a risk has been accepted, it should be kept under frequent review in case the circumstances of the risk or the availability of appropriate controls should change.

7.3 Transferring the Risk

If an organisation finds it too difficult or too expensive to amend exiting controls or implement new ones to reduce risks to an acceptable level, it may consider transferring the risk to a third party who is better positioned to manage the risk effectively. The most common example of risk transference is the use of insurance: taking out an insurance policy may not reduce the possibility of the risk occurring, but an appropriate policy will reduce the impact on the business. Insurers may not cover every eventuality, or there may be conditions or excesses that apply (see Section 6.5).

Another alternative for transferring unacceptable risks is to consider the use of appropriately qualified and suitably equipped third parties such as outsourcing providers (for example, in the provision of secure data centre services). In this scenario, additional controls which provide for the provision of effective security in outsourcing agreements and supporting SLAs should be in place with the third party. As the originating organisation maintains primary responsibility for managing the risk, any elements which cannot be fully outsourced should be considered as residual risks (see Section 6.5), including consideration of any new risks which may arise out of the act of outsourcing.

7.4 Avoiding the Risk

One of the simplest options for managing unacceptable risk is to avoid the risk altogether. Normally this involves the stopping of certain types of business activity (for example, not conducting sensitive business over public internet connections) or relocating assets (for example, moving assets away from an area identified as being in a flood zone). However, it is not always possible for an organisation to simply stop undertaking certain types of activity whilst continuing to carry on business as normal.

7.5 Managing Residual Risk

Whenever an unacceptable risk is either reduced, transferred or avoided, there will frequently be some element of residual risk remaining. A risk assessment of this needs to take place to ascertain whether the residual risk falls within the organisation's level of acceptable risk (set by Executive Management in Section 1):

- if it does, then the risk is acceptable, and no further action is required at this time
- if it does not, consideration should be given to implementing further risk treatment options
- if no further risk treatment options are available, risk acceptance will be required

8.0 Establishing an Inventory of Assets

(ISO/IEC 27002:2013, Control A8.1.1)

8.1 Information Assets

Having defined the scope of the ISMS in Section 2, it is now necessary to identify all the information assets (data sources) that fall within this scope. It may help to approach this task by considering all the different types of information that exist in different areas of the business, for example:

- Operational data (e.g. password databases, firewall configurations, audit logs)
- Financial data (e.g. budgets and forecasts, debtor and creditor records)
- Commercial and legal data (e.g. contracts and service level agreements)
- Sales and marketing data (e.g. sales proposals, fact sheets, white papers)
- Client specific data (as supplied by clients as being trusted to the organisation)
- Personnel/HR data (e.g. personal information, salary details, pension arrangements)
- Don't overlook data that may be entrusted to third parties (e.g. off-site payroll bureau)

These should be compiled into a table, so that for each information asset the following details are recorded as a minimum:

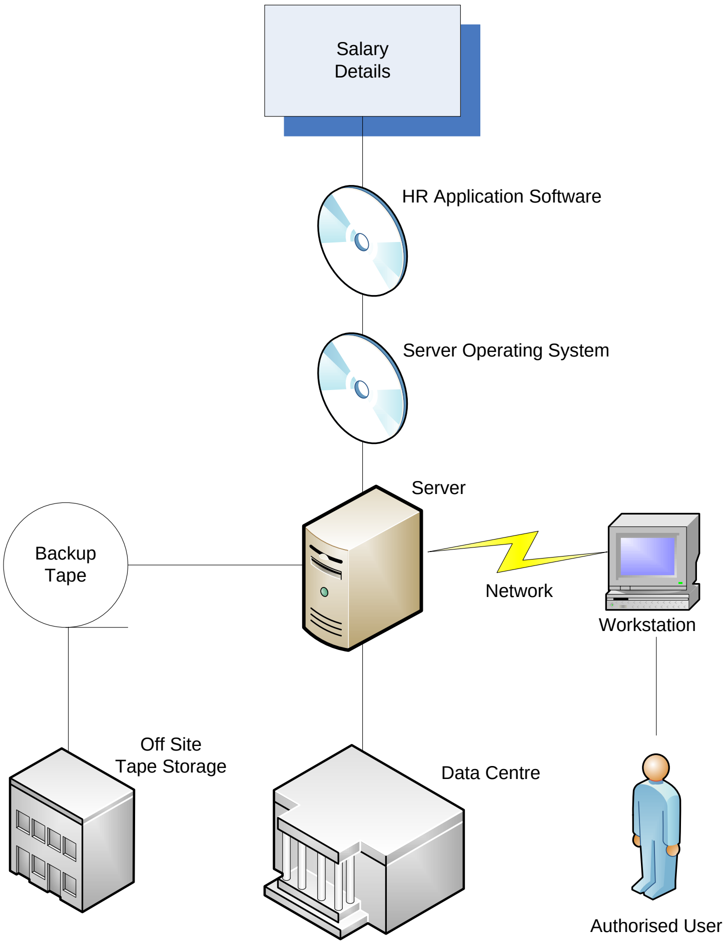
- Asset name
- Asset location and format (e.g. paper records, electronic file etc.)
- Asset owner (named person, ultimately responsible for the security of the asset)
- Date of last asset risk assessment
- Result of last asset risk assessment (e.g. clear, risk treatment, risk acceptance etc.)
- Frequency of planned asset risk assessments (e.g. every 12 months)

At this point, an Information Asset Evaluation would take place (see Section 8) to understand whether the information asset is of enough criticality or sensitivity to require a full risk assessment, or whether it is of lesser importance and the use of standard "baseline controls" would be more appropriate (see Section 12/Appendix A). For those information assets assessed as being critical and/or sensitive, and hence requiring a full risk assessment, it is very important to identify, record and assess the "supporting assets" upon which they also depend for their security.

8.2 Supporting Assets

As noted previously, information assets cannot be considered in isolation. It will be necessary to identify those supporting assets upon which information assets rely for their security: examples will include buildings, computer hardware, computer software (both operating systems and applications), networks, mobile devices and back-up media.

As a simple example, consider the information asset of salary details with an organisation:



Example of Information Asset and Supporting Asset Dependencies

Even in this simple example, it can be observed that the salary details are controlled by the HR application, which resides on a server with an operating system. The server lives in a data centre, with network connectivity to desktop computers accessed by authorised users. The data is also backed up from the server onto a back-up tape, which is taken off-site and stored in a separate facility. To ensure the total security of the salary information, it is necessary to understand the vulnerabilities and threats to the other supporting assets detailed above.

It is, therefore, extremely important to understand the relationship between an information asset and its supporting assets, and, therefore, the relationship between different supporting assets (in the above example the server is reliant upon the physical security provided by the data centre).

Some organisations undertake risk assessments on "people" as a standalone exercise, assessing issues such as skills shortages, theft, social engineering, acceptable use policy compliance etc. Others do not recognise "people" as an asset in their own right, rather they choose the more integrated approach of including people-based risks as threats to the appropriate supporting asset – e.g. theft of media (in a media risk assessment), unauthorised access to premises (in a building risk assessment), interception of email messages (in an information risk assessment) etc. Both approaches are valid, although the second requires a more detailed understanding of the potential threats that employees, contractors and end-users have on different types of assets.

9.0 Information Asset Evaluation

(ISO/IEC 27001:2013, Section 6.1.2)

Not all identified information assets will be of sufficient value or sensitivity to the business to necessitate a detailed risk assessment exercise. Having compiled the Information Asset Inventory, an initial assessment of all included data should be undertaken:

9.1 Confidentiality Assessment

What would be the impact on the organisation of a breach of confidentiality of this specific information asset – e.g. if it became available to competitors, clients or the press?

9.2 Integrity Assessment

What would be the impact on the organisation of a breach of integrity of this specific information asset – e.g. if it were to become corrupted, hacked, or in some other way unreliable for business use?

9.3 Availability Assessment

What would be the impact on the organisation of unavailability of this specific information asset – either short term (define, perhaps a few hours) or long term (define, perhaps a few days or more)?

For each of these questions, the answer could be a numeric value, as follows:

0 no impact, business would not be affected in any way

1 very limited impact, business would be only slighted affected by the breach

2 some impact, business would be inconvenienced by the breach but not critically

3 significant impact, the ability to continue normal business is affected somewhat

4 serious impact, normal business operations would be interrupted

5 major impact, the continuing operations of the business are threatened

By this stage, Executive Management has already decided upon the organisations acceptable risk levels. One of the decisions taken should be to understand which information assets should be escalated to full risk assessment, based upon this high-level risk assessment. It is for the organisation to choose what level is acceptable. Full risk assessments are detailed below.

Access Intelligence has decided that any single question answering 3 or higher requires a full risk assessment.

Important: if an information asset is identified as requiring a full risk assessment, all the supporting assets upon which it defends should be subject to a full risk assessment too. Only by doing this can the total threat landscape of the information asset be fully understood. It will probably be the case that supporting assets may support the security of more than one information asset, but they would normally only be assessed once, regardless of how many information assets depend on them. As an example, a data centre would be assessed once for unauthorised entry, one for controls against fire etc. and these assessments of threats would in turn apply to all servers housed in the facility.

10.0 Full Asset Risk Assessments

(ISO/IEC 27001:2013, Section 6.1.2)

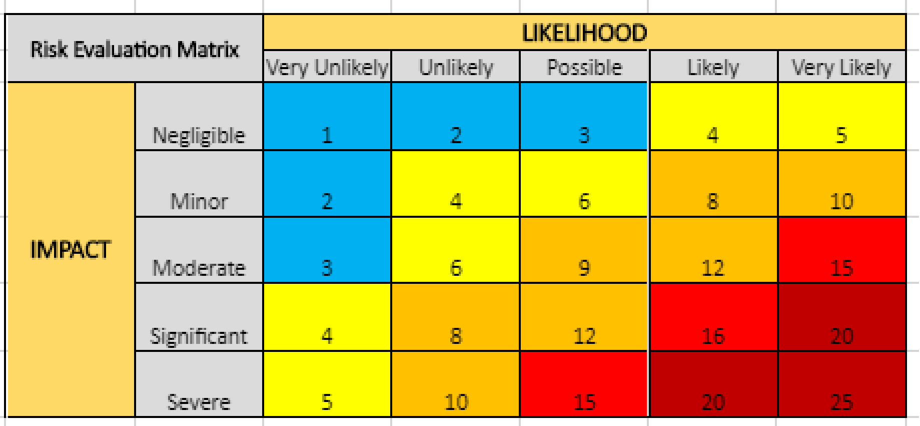
In a full risk assessment, each identified information or supporting asset will be assessed by its assigned asset owner against the specific threats and vulnerabilities that could affect or compromise it. Different types of asset will be subject to assessment against different types of relevant threats: let us look at two examples:

- Theft: it is extremely difficult to steal a building, although much easier to steal a laptop
- Flooding: does not affect software code in isolation, although it is likely to affect the premises, hardware and media upon which the software may be stored

One of the most important elements of undertaking effective risk assessments is to identify and focus on the specific threats and vulnerabilities that are likely to affect the asset being assessed. Consequently, it is common for risk assessment methodologies to suggest using different risk assessment “templates” tailored to each asset category.

The asset owner, using their knowledge of the asset, will be able to identify all existing controls that are in place to prevent or manage the opportunity for a vulnerability to be exploited by a threat, and document these.

With the current controls in place, the asset owner will assess the probability of the threat actually happening and assess the impact on the organisation if it did. This information will typically be assessed against a standard 5 x 5 risk matrix, for example:

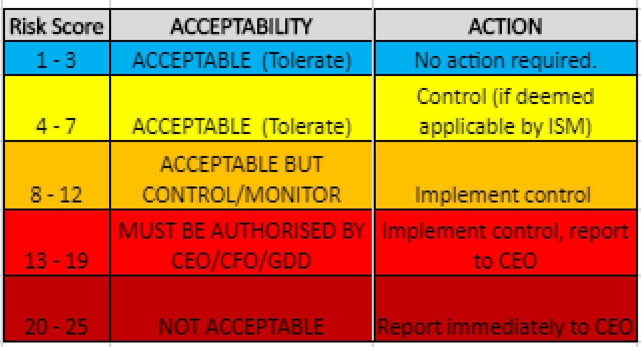


Risk Evaluation Matrix		LIKELIHOOD				
		Very Unlikely	Unlikely	Possible	Likely	Very Likely
IMPACT	Negligible	1	2	3	4	5
	Minor	2	4	6	8	10
	Moderate	3	6	9	12	15
	Significant	4	8	12	16	20
	Severe	5	10	15	20	25

Back in Step 1, the Executive Management agreed what would be the acceptable risk level for the organisation. In the above 5 x 5 risk matrix, it could be as prescriptive as “any risk of higher than 12 is unacceptable” or more general such as “any risk coloured red or dark red is unacceptable”.

Should any risks be found to be unacceptable, it indicates that the current implementation of security controls is not appropriate to the organisation’s risk profile, and the controls are not providing effective protection to the asset concerned.

Risk acceptability and actions prescribed by Access Intelligence:



Risk Score	ACCEPTABILITY	ACTION
1 - 3	ACCEPTABLE (Tolerate)	No action required.
4 - 7	ACCEPTABLE (Tolerate)	Control (if deemed applicable by ISM)
8 - 12	ACCEPTABLE BUT CONTROL/MONITOR	Implement control
13 - 19	MUST BE AUTHORISED BY CEO/CFO/GDD	Implement control, report to CEO
20 - 25	NOT ACCEPTABLE	Report immediately to CEO

Unacceptable risks should be treated using one (or more) of the risk treatment activities described in Section 7. The most common approach is to examine and improve existing controls, either by supplement existing controls with new controls, or replacing weaker controls with newer, stronger or more appropriate ones.

Risk Priority by Access Intelligence:

- Highest = Dark red / risk score of 20-25
- High = Red / risk score of 13-19
- Medium = Orange / risk score of 8-12
- Low = Yellow / risk score of 4-7
- Lowest = Blue / risk score of 1-3

Once the selected risk treatment activity has been completed, the risk assessment should be re-visited: if the risk treatment has been successful the risk should now be within the range of acceptable risks for the business.

If, however, it remains unacceptable further risk treatment activities will be required. This cannot continue indefinitely – at some point the organisation may reluctantly have to accept the risk and document its reasons for doing so.

All unacceptable risks should be documented within a "Risk Treatment Plan", including:

- Which threat(s) are considered to be putting the asset at unacceptable risk.
- Which controls are already in place, relevant to the threat being reviewed.
- The method of risk treatment (accept/reduce/transfer/avoid) – as per Section 6.
- Which new or amended controls are proposed.
- The period necessary to implement new or changed controls.
- A sign off when the threat has been treated.
- Many organisations compile Risk Treatment Plans into a central Risk Treatment Register.

11.0 The Statement of Applicability (SOA)

(ISO/IEC 27001:2013, Section 6.1.3 d)

ISO/IEC27001:2013 requires a documented "Statement of Applicability" detailing both the control objectives and the individual controls that have been selected when administering the organisation's ISMS. Typically, this will be extracted from the completed set of risk assessments and will detail by control objective and control (from Annex A of ISO27001), which assets are using that control during the current risk assessment period, and the reasons for that use.

Controls may be selected:

- As a result of their selection by a detailed (full) risk assessment
- As a result of them being considered a "baseline control" for non-critical information assets
- As a result of them being an integral part of the operation of the ISMS
- As a result of contractual requirements

12.0 Ongoing ISMS Activities

(ISO/IEC 27001:2013, Sections 7, 8, 9 and 10)

12.1 Information Security Training

The ISO27001 standard details how training, awareness and competence are to be achieved for personnel engaged with operating or participating in the ISMS. This should be conducted in accordance with the organisation's Information Security Training Policy (see **ISDL02**) and should consist of initial induction training with messaging reinforced by periodic refresher training.

There is a need to record that such training has taken place and for its effectiveness to be evaluated – these are mandatory requirements of the Standard.

12.2 Internal Audits

Organisations should conduct regular internal audits to ensure that ISMS related policies, processes, procedures and controls are effectively implemented and performing as expected. This is a formal requirement of ISO27001, and external auditors routinely check the contents of internal audit reports.

Internal audits should be undertaken by suitably qualified auditors not connected to the activity or processes being audited. They should be planned in advance, with the criteria, scope, frequency and approach agreed, taking into consideration the status of the activity or process being assessed as well as the results of any previous audits that have taken place (see **ISDL14** for more information).

Should any non-conformances be identified, it will be necessary to arrange a follow-up session to ensure that effective corrective (and preventive) actions have been implemented so as to address the non-conformances fully. Executive Management should review internal audit reports.

12.3 Management Review

Executive Management has a responsibility to review the ISMS. This includes reviewing internal audit reports (see Section 11.2) and the results of risk assessments. The main act of management review is the formal ISMS review, which should take place at planned intervals in accordance with the Management Review Policy (see **ISDL09**). This session should ensure that the ISMS continues to be suitable for the organisation, including the Information Security Policy (see **ISDL01**) and all current information security objectives.

12.4 ISMS Improvement

An organisation should strive to continually improve its ISMS through the use of a variety of measures, including implementing corrective and preventive actions in response to internal audit reports and information security incidents. Improvement opportunities also arise from the results of risk assessments, especially where risks are identified which exceed the organisation's defined limit of acceptance.

Formal management review presents the opportunity of assessing the performance of the ISMS, and may trigger improvement events such as policy amendments, the implementation of new or amended security controls, or the provision of general or focussed employee training plans.

13.0 ISMS Documentation & Records

13.1 Policies, Processes and Procedures

ISO27001 specifies a number of mandatory documents that need to be created and implemented in order to meet the requirements of the Standard. This, however, is by no means the minimum that an organisation needs to operate an effective ISMS or progress to certification: additional policies, processes and procedures will be required to address specific information security requirements and to manage, implement and measure controls.

13.2 Records

ISO27001 specifies a number of mandatory records that need to be created and retained in order to demonstrate compliance with the requirements of the Standard. This, however, is by no means the minimum that an organisation needs to operate an effective ISMS or progress to certification: additional records will be required to illustrate management decisions, review meetings, control effectiveness measurements, etc. Records also need to be created and updated with regard to the ISMS objectives, to record and demonstrate progress made and objectives achieved.

14.0 Appendix A: Baseline Security Controls

In Section 8, the organisation performed an Information Asset Evaluation, and identified those information assets that were considered to be of a sensitivity or criticality where a full risk assessment should take place (as detailed in Section 9). Many organisations consider that every information asset, regardless of its assessed sensitivity or criticality, should be subject to a "baseline set" of security controls, in the interests of good information security best practice.

The following list should be considered as a sensible starting point for establishing a set of baseline controls that should apply to every information asset within an organisation. For information assets that require a full risk assessment, each of the controls below should be available for selection against the appropriate threat within the full risk assessment template (for example, the risk of an authorised change can be controlled by, amongst other things, acceptable use of assets and information security training). For those information assets that do not require a full risk assessment, the asset owner should be asked to sign their agreement to the baseline controls being in place and providing appropriate safeguards for their specific assets.

As a starting point, an organisation may consider the following as suitable baseline controls:

- Information Security Policy Document (A5.1.1)
- Review of Information Security Policy (A5.1.2)
- Allocation of Information Security Responsibilities (A6.1.1)
- Confidentiality Agreements (A13.2.4)
- Independent Review of Information Security (A18.1.1)
- Inventory of Assets (A8.1.1)
- Ownership of Assets (A8.1.2)
- Acceptable Use of Assets (A8.1.3)
- Classification Guidelines (A8.2.1)
- Information Labelling and Handling (A8.2.2)
- Roles and Responsibilities (A6.1.1)
- Screening (A7.1.1)
- Terms and Conditions of Employment (A7.1.2)
- Personnel – Change or Termination of Employment (A7.3.1)
- Management Responsibilities (A7.2.1)
- Information Security Awareness, Education and Training (A7.2.2)
- Disciplinary Process (A7.2.3)
- Reporting Information Security Events (A16.1.2)
- Reporting Security Weaknesses (A16.1.3)
- Responsibilities & Procedures for Security Events (A16.1.1)
- Identification of Applicable Legislation (A18.2.1)
- Protection of Organisational Records (A18.2.3)
- Data Protection & Privacy of Information (A18.2.4)
- Compliance with Security Policies and Standards (A18.1.2)

Baseline Controls should be detailed separately within the Statement of Applicability.

15.0 Document Control

This manual needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this manual, for example as a result of a reported information security incident, formal review or an audit finding.

- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document

- A change in the way which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the accuracy of this document

The current version of this manual, together with its previous versions, shall be recorded below.

Version History

Revision	Author	Date	Reason for issue
1.0	David Roud	31/10/2018	First version, to enable Access Intelligence to achieve ISO 27001:2013 accreditation
2.0	Ato Abraham	26/11/2019	Amendments made in preparation for Stage 1 ISO 27001 audit
3.0	Adam Palmer	20/01/2021	Added Patch Management to policy. ISO 27001 certification was achieved in June 2020. Policy re-formatting.
4.0	Adam Palmer	22/11/2021	Mitigation timeframes

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer	MFautley	22/01/2021
Mark Fautley	**Chief Financial Officer**	MFautley	**20/01/2022**