Telstra Limited trading in EMEA as Telstra Global. This document applies to Telstra Limited referred to throughout as Telstra Global.

Summary

This document describes the Telstra Global Information Security Management System (ISMS) framework. It summarises the key roles and responsibilities and activities undertaken to facilitate continual improvement.
**Contents**

<table>
<thead>
<tr>
<th>#</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>02</td>
<td>Scope of the ISMS</td>
<td>5</td>
</tr>
<tr>
<td>03</td>
<td>Telstra Global's Policy and Associated Objectives</td>
<td>7</td>
</tr>
<tr>
<td>04</td>
<td>Telstra Global's Organisational Framework</td>
<td>9</td>
</tr>
<tr>
<td>05</td>
<td>Resource Management</td>
<td>13</td>
</tr>
<tr>
<td>06</td>
<td>How does Telstra Global manage information security risk</td>
<td>14</td>
</tr>
<tr>
<td>07</td>
<td>Compliance Management</td>
<td>15</td>
</tr>
<tr>
<td>08</td>
<td>How Telstra Global Manages, Measures and Improves</td>
<td>16</td>
</tr>
<tr>
<td>09</td>
<td>Documented Information</td>
<td>21</td>
</tr>
<tr>
<td>10</td>
<td>Change History</td>
<td>23</td>
</tr>
</tbody>
</table>
01 Introduction

Telstra Global is committed, in accordance with its company purpose and values, to maintaining and improving information security and business continuity and minimising exposure to risk within the company to provide and support managed hosting and network services including international data services to customers worldwide.

1.1. The Organisation

- Telstra Global EMEA provides and supports managed hosting and network services including international data services
- Telstra’s portfolio is complemented by its independently-owned and managed switched UK network. The network incorporates strategic Points of Presence (PoPs) across EMEA, including data centres located in London - Docklands, London - Woking and Cambridge, and interlinks seamlessly with Telstra’s Global Next IP™ managed network
- Telstra Global EMEA has 150 employees across two offices in London and Cambridge. Telstra Global EMEA is aligned to selling the Telstra Global Product Portfolio of network solutions, hosting solutions and a range of telephony services
- Telstra Global EMEA has two hosting centres:
  - London Hosting Centre - Docklands is located in Canary Wharf the LHC is 114,250 square foot with approximately 1,800+ racks. The site supports a variety of services including fully managed services and co-location suites.
  - London Hosting Centre - Woking is a three-storey building in Surrey which houses 935m² of technical hosting space. The building has been designed to meet the needs of Telstra’s customers, who can be certain that their business critical systems are co-located in fully redundant facilities with excellent standards of service and maintenance.
  - Both hosting centres are supported 24 hours a day by on-site security and maintenance teams.
- Telstra Global EMEA is part of Telstra Global which is a division of Telstra Corporation Limited, Australia’s leading and largest telecommunications and information-services-company.
1.2. Telstra Corporation

- Telstra is Australia's leading telecommunications and information services company.
- Together with its offshore subsidiaries and international investments, Telstra serves over 200 of the world’s top 500 companies, spanning Europe, Asia-Pacific and the Americas.

1.3. Telstra International Group (TIG)

- TIG is a leading global supplier of managed network services and a division of the leading Australia-based, tier 1 telecommunications and media services company, Telstra Corporation Limited. Telstra owns one of the most technologically advanced IP backbone networks in the world.
- Headquartered in Hong Kong, TIG is responsible for managing Telstra's assets outside Australia. This includes CSL – a leading Hong Kong mobile operator, China-based digital media services and Telstra Global, a network and managed services business.

1.4. Telstra Global

- Telstra Global is a leading global supplier of managed network services and international data, voice and satellite services.
- Telstra Global provides innovative and flexible global communications and IT services and solutions for organisations looking to maximise the benefits of globalisation, and expand to, in and from growth regions such as Asia, whilst driving sustainable growth and enhancing business agility.
- Telstra Global has licences in most major Asian markets and facilitates access to over 1,400 PoPs in 230 countries and territories across the globe.

1.5. Customers Suppliers and Other Interested Parties

Telstra Global has identified a number of parties that have an interest in the, activities and products and services that we provide.

As well as the organisations within the Telstra Group Telstra Global has a number of different types of customer, relationships with suppliers and various other interested parties.
02 Scope of the ISMS

The scope for the Information Security Management System (ISMS) covers:

‘The provision and support of managed hosting and network services including international data services provided by Telstra Global (EMEA)’

This scope includes the management of services provided by the company and supported by third parties (e.g. service providers, business partners and subcontractors).

It includes all activities that hold, obtain, record, use, share or manage employees, corporate, client information or data.

2.1. Services

- Managed Services
- Colocation Hosting Services (including remote eyes and hands)
- Network Services (including professional services)
- Hostmaster services

2.2. Activities

Activities undertaken to provide these services are grouped into the following areas:

- Sales & Marketing
- Technical Implementation
- Operations
- Finance
- Human Resources and Office Facilities
- Technical
- Project Management

2.3. Information

The ISMS protects information held on or processed within IT systems, this includes information about:-

- Building Access and Management Information
- CCTV Images
- Commercial Information
- Compliance Information
- Contractual Information
- Corporate Governance
- Customer Billing Information
- Customer Information
- Customer Technical Information
- Customer’s Data
- Electronic Access Information
- Employee Information
- Financial Information
- Hostmaster Information
- Marketing Collateral
- Legal Information
- Policies, Processes and Procedures
- Product Information
- Marketing Information
- Sales Pipeline
- Supplier Contractual Information
- Technical Drawing / Configuration
- Tender Information
2.4. Locations
All services and activities are undertaken in the following locations

- Blue Fin Building
- LHC London
- LHC Woking

2.5. Corporate Applications
The Applications used to include the services provided include

- Financial Systems
- Customer Relationship Management
- Operations Support Systems (OSS)
- Business Support Systems (BSS)
- HR Systems
- Office Systems

2.6. Monitoring Tools Dependencies
The activities undertaken are dependent on services provided a variety of other Telstra Locations and Entities:

- Cambridge Data Centre
- Points of Presence (POPs)
- Telstra International (Sydney, Hong Kong)

The activities undertaken are dependent on services provided a variety of suppliers and service providers:

- Data Centre facilities (Landlord, Managed Services, Security) Cleaning, Maintenance Contractors others)
- Office facilities (Landlord, Security Cleaning, Maintenance Contractors others)
- Network and Telephony Connectivity service providers / carriers (leased lines)
- Installation Service Providers (e.g cable installation)
- Desktop support services
- SaaS Service Providers

Local Supplier registers list provide full details.

Assurance of the effective implementation or operation of activities and controls carried out by the relevant third parties will be achieved by a combination of formal contracts, service level agreements (SLAs), service monitoring, performance reporting (against agreed key performance indicators) and independent audits.

2.7. Interested Parties
Telstra Global has identified a number of parties that are interested in this ISMS. Their needs and expectations have been identified, taken into consideration and documented during the development of this ISMS.

2.8. Exclusions
All clauses of ISO 27001 are included within the scope of the ISMS.

The controls selected within the ISO 27001 Annex A, have been listed in the Statement of Applicability

The activities undertaken by Telstra Global are dependent on services provided a variety of service providers:
03 Telstra Global's Policy and Associated Objectives

3.1. Leadership and Commitment

Telstra Global’s Senior Management Team (SMT) will demonstrate by example their commitment to the principles of the ISMS. They will individually and collectively ensure that:

- Direction and support is given to all employees and people leaders to ensure that they can contribute effectively to the ISMS
- All people leaders and SIRT members are given the support and authority to allow them to lead within their areas of responsibility in relation to Information Security
- The Information Security Policies and this ISMS Framework are communicated to everyone in the organisation
- The requirements of interested parties, including customer, as well as statutory and regulatory requirements are adhered to as part of any activity where commercially viable and technically feasible.
- Meaningful, measurable and achievable ISMS objectives are set and their effectiveness monitored to ensure that the intended outcomes are achieved
- Information security will be included in corporate strategic plans.
- Improvement is an integral part of the aims and objectives of the Company.
- Regular management reviews are conducted as determined and defined.
- Adequate and suitable resources are provided and made available to match the business need and longer term strategic plans.
- The facilities and working environment are suitably maintained to aid the development and continual improvement of Telstra Global.

3.2. Information Security Policy

An Information Security Policy has been created and authorised by the Chief Executive Officer (CEO) All other policies and processes have been created and authorised by the Security Incident Response Team (SIRT) and relevant owners.

These policies and processes have been communicated to all users and are freely available on the Telstra Global EMEA DMS.

The policies are communicated to all employees at induction to ensure that they understand the responsibility of working together to achieve the policies’ aims and objectives.

The suitability and relevance of these policies are reviewed at least annually.

3.3. ISMS Objectives

To support the ISMS, the information security objectives shall be set and defined. The SIRT will review these objectives annually, and key performance targets will be identified and subsequently monitored, measured and reported. These objectives and KPIs will be reviewed and approved by the SMT

The effectiveness of the set objectives and targets are assessed and monitored by the:

- Assessment of information from measurement, monitoring and inspection activities.
- Analysis of internal performance, and customer feedback information.
- Review of audit activities
3.4. ISMS Implementation

In order to achieve the Company’s objectives and demonstrate to clients, potential clients, partners and Telstra Global’s target market, Telstra Global’s commitment to providing quality services, while protecting their information, Telstra Global is implementing an ISMS which complies with ISO 27001. This means that:

- The needs and expectations of Telstra Global’s customers, suppliers and other interested parties will be clearly defined and verified through documentation and reviews
- A variety of policies, processes, procedures and standards will be planned, created, approved, implemented, controlled and reviewed regularly to support the policy
- The ISMS will be risk assessed and the risks and opportunities that are identified will be addressed to ensure that the ISMS meets its intended objectives
- The effectiveness and efficiency of the ISMS will be reviewed via independent internal audits, performance monitoring, management reviews
- Training and development needs for corporate or individuals will be identified and will be available to all employees
- All non-conformances and issues will be reported to and investigated and suitable action will be taken in a timely manner
- Where the development or acquisition of products, services or processes has been outsourced to third parties, the management of Information Security will be controlled through suitable contracts, service level agreements, definitions of requirements, deliverables monitoring, product or service acceptance procedures and audits
4.2. ISMS Roles & Responsibilities

This section summarises authority levels and roles specific to the ISMS.

All employees have a formal job description defining their roles and responsibilities (R&Rs). This is reviewed by line management at least annually. Changes in the scope of roles and responsibilities are to be captured by the relevant department head as part of the relevant process. R&Rs support the ISMS in defining WHO is meant to be competent to do WHAT.

4.3. Employees

All employees have overall responsibility for:

- Ensuring they fully understand and execute their responsibilities under the ISMS
- Ensuring that they know and understand the company policies, that they adhere to the best practice processes and work securely
- Reporting any information security incidents or weaknesses to the SIRT
- Informing their People Leaders of any security related issues or concerns.
4.4. People Leaders

People Leaders are responsible for ensuring:

- the implementation of the ISMS within their own team and suppliers, ensuring that all applicable policies, processes and standards are followed within their area
- that any outstanding agreed actions related to the ISMS are completed promptly

People Leaders need specifically to:

- Ensure they know, understand and execute the ISMS
- Ensure employees know and understand the ISMS and their specific responsibilities
- Ensure all suppliers, service providers and contractors know and understand the relevant aspects of the ISMS and their specific responsibilities
- Communicate with other people leaders and the SIRT with regard to information security and business continuity issues
- Resolve conflicts within their areas of responsibility
- Identify improvement initiatives within their areas of responsibility
- Approve significant document changes (and all process changes)
- Allocate reviewers for document changes, and assume default responsibility for reviewing documents
- Ensure employees adhere to best practice and work securely
- Escalate any major security incidents, complaints or non-conformances directly to the SIRT.

4.5. Sales Team / Customer Operations Team

The Sales Team and Customer Operations Team are responsible for:

- Maintaining customer focus by ensuring customer security and business continuity management requirements are determined and met, therefore enhancing customer satisfaction
- The point of contact for customers and is responsible for ensuring customer requirements are made explicit and agreed.
- Day to day responsibility for ensuring the satisfaction of their assigned customers and ensuring complaints / incidents are escalated to the appropriate level of management.
- Ensuring that any customer requirements that conflict with Telstra Global Policy are discussed and approved with the SIRT prior to entering into an agreement with a customer.

4.6. Policy and Process Owners (also likely to be People Leaders)

For each relevant policy and process the ‘owners’ are responsible and accountable for:

- Being publicly and formally recognised as ‘the owner’
- Effective communication both internally and externally
- Ensuring its alignment with strategic objectives
- Ensuring it is fit for purpose (or introducing an alternative)
- Developing it and being alert to end-of-life planning or reinvention
- Ensuring regular reviews takes place to confirm its fitness for purpose
- Policing to ensure appropriate adherence and appropriate use
• Ensuring ongoing monitoring and analysis to confirm it is applied as designed and is effective
• Ensuring any identified corrective actions and / or improvements are applied in a timely manner
• Defining its ‘criticality’ for the purposes of information security and business continuity management
• Managing related incidents affecting areas of ownership
• Ensuring all supporting documents and records are well controlled in line with company practice
• Ensuring the provision of adequate training and awareness about policy / process
• Managing risks as relevant to their process
• Escalating issues and providing performance summaries as requested to SIRT

Coordinating information security initiatives, including maintaining contact with the relevant authorities and special interest groups in their area of responsibility.

4.7. Security Incident Response Team (SIRT)

The Chief Operating Officer EMEA is ultimately responsible for the provision of all resources to ensure an effectively implemented ISMS in order to achieve objectives.

The SIRT champions and fully supports the implementation of the ISMS, including resolving any escalated issues and facilitating the management reviews of the ISMS.

Overall responsibility and ownership of the ISMS includes:
• Setting, reviewing and communicating the information security objectives
• Addressing issues of major importance on information security
• Ensuring a secure working environment
• Defining responsibilities and authorities
• Communicating responsibilities and authorities to the organisation
• Ensuring the provision of adequate and suitable training and leadership
• Ensuring the efficient and effective use of all resources, including the availability of resources for ISMS activities
• Communicating and reporting to the business any key messages and important issues of information security and business continuity
• Ensuring all managers are appropriately trained and competent in information security and business continuity leadership
• Ensuring clear direction and visible management support for ISMS initiatives
• Authorising any changes to this ISMS framework.

4.8. Compliance and Standards Project Manager

The Compliance and Standards Project Manager is responsible for monitoring the working ISMS to ensure it meets the requirements of ISO 27001. Specific responsibilities are:
• Ensuring policies and processes needed within the ISMS are implemented and maintained
• Reporting to the management on the performance of the ISMS and any need for improvement
• Ensuring communication takes place regarding the effectiveness of the ISMS
• Providing guidance on the implementation of the ISMS
• Managing the ISMS programme
• Facilitating the SIRT meetings and Management Reviews
• Managing the release of all changes to the ISMS
• Monitoring and measuring the effectiveness and efficiency of the ISMS
• Managing and monitoring corrective, preventive and improvement actions through the continual improvement programme
• Encouraging the implementation of policy and process improvement activities throughout the organisation, by effective methods of communication and the employment of good working practices
• Highlighting issues relating to the effectiveness of the ISMS and any areas of concern for immediate review and action.

4.9. Internal Communication

All relevant information regarding delivery of the security objectives will be shared with the appropriate individuals, in a suitable format (e.g. meeting, conversation, email, document circulation, conference call, briefing, etc.).
05 Resource Management

Telstra Global management has committed to reviewing and supplying the relevant resources that are needed within the Company to support establishment, implementation and continual improvement of the ISMS. This includes:

- Resources needed to manage the ISMS and facilitate the implementation of internal policies and processes.
- Resources needed to implement the policies and processes of the ISMS
- Infrastructure requirements such as building improvements and equipment.
- IT Infrastructure requirements such as network, systems and desktops.

The justification to provide resources will be dictated by the business needs, to maintain compliance with the requirements of customers and other interested parties, to improve the efficiency and capability, to remain competitive and to ensure conformance to the ISMS.

Telstra Global ensures adequate resources are provided, by undertaking resource planning both on an annual and project basis.

5.1. Human Resources

Human resources are strategically planned on an annual basis with all new requirements being identified, implemented, and monitored throughout the year, where relevant.

Telstra Global is committed to recruiting personnel with appropriate skills and competence (based on appropriate education, training or experience).

Telstra Global is committed to ensuring that its personnel have been provided with suitable and sufficient training to ensure that all its employees are equipped with the required skills and knowledge to carry out their respective tasks.

5.2. Building, Data Centres, IT and Network Infrastructure

Maintaining the infrastructure of Telstra Global is the overall responsibility of the Chief Operating Officer EMEA, delegated down to the respective People Leaders. They have the responsibility for ensuring their particular work areas, equipment, and support services are maintained to the standard that will achieve service conformity and security.

5.3. Supplier Management

It is policy to maintain a supplier list (including subcontractors and service providers). An assessment of the suppliers is carried out before agreeing the contract and details of the requirements for the specific standards to be followed will be agreed and documented as part of the contract.

Where information is accessed, stored, processed, distributed or archived by a supplier a risk assessment is carried out and mitigating controls are implemented to reduce any identified risks.

Telstra Global aims to build partnership relationships with its suppliers and will work with them to build confidence in the security of the services they are providing.

Audits of suppliers are included in the audit programme, their need and frequency determined by the level of risk with each supplier.

5.4. Supporting Material

- HR, Building and IT resource plans and budgets,
- HR Security controls such as references, identification verification records, contracts,
- IT and Building security controls
- Operating level agreements for other Telstra services
- Supplier Management Policy
- Supplier Register, Contracts and Service Level Agreements
- Service Review Minutes, Audits and Assessments
06 How does Telstra Global manage information security risk

6.1. Information Security Risk Management

The implementation of this ISMS requires that Telstra Global conducts a robust programme of risk management as a means of determining and confirming the appropriateness of information security related controls for Telstra Global’s systems and services.

A systematic approach to operational and information security risk management is necessary to identify business needs regarding operations, information security and business continuity requirements (including contractual and regulatory) and to create an effective ISMS.

Risk management is not a one-off exercise with a single set of control recommendations which remain static in time, but a continual process. During the operational delivery and maintenance of the live production, there will be a number of instances where risk assessment activity will be necessary.

Telstra Global has applied The Abriska Methodology in accordance with its Information Security Risk Management Policy.

6.2. Statement of Applicability

The Statement of Applicability list all controls that have been selected and identifies whether the control is fully or partially implemented in relation to the requirements of the control objectives. Reasons for selecting controls are documented as part of the risk assessment process. The justification for controls that have not been selected will be documented with the Statement of Applicability.

6.3. Ongoing Risk Management

Ongoing management of risks will be controlled by information received from incident reports, audit results, technical advisories and confirmed or potential technical or process vulnerabilities.

The SIRT and the Compliance and Standards Project Manager are responsible for ensuring that changes to the organisation, its technology, business objectives, processes, legal requirements and identified threats are incorporated into the ISMS.

Where appropriate, the Compliance and Standards Project Manager will initiate the risk assessment process to ensure that all controls are relevant.

The SIRT can if required implement additional controls without undertaking a risk assessment, if the threat or vulnerability could have a significant impact on the organisation, its partners or personnel.

The Compliance and Standards Project Manager will maintain a Risk Assessment Programme (part of the ISMS Programme) to ensure that all major information assets, third parties and major information systems undertake at one risk assessment within a 3 year cycle.

All changes to the ISMS will be reviewed at the Management Reviews and documented within the minutes.

6.4. Supporting Material

The following materials support this activity

- Information Security Risk Management Policy
- Supporting policies and processed resulting from the risk assessment

The following records are maintained:

- Risk Assessment Programme
- Information Security Asset List, Business Impact Analysis, Risk Analysis and Reports, Risk Treatment Plans, Risk Acceptance Requests
- Statement of Applicability
07 Compliance Management

7.1. What is Compliance Management

A set of activities undertaken to ensure that the organisation had identified and is compliant with all requirements. There are a number of compliance requirements defined for Telstra Global.

7.2. Information Security Management System

The management system in place is compliant with the ISO 27001 Standard. An internal audit programme is established annually to ensure continued compliance, including external audits by a third party.

7.3. Identification of Legal, Regulatory & Contractual Requirements

The high-level policy states that, legislative requirements will be adhered to therefore Telstra Global’s will review all contracts, as well as any applicable legal and regulatory requirements to ensure the Company is able to comply with any such requirements. Where necessary, the Legal Department will liaise with appropriate process owners to facilitate any information security requirements.

A register of all requirements is maintained and reviewed annually.

Should other relevant laws be passed, they will be reviewed and actions taken as necessary to ensure compliance.

7.4. Evidence of Compliance

To demonstrate ongoing compliance with the ISMS, all supporting documents and records (as listed in the document and records management section of this document, and/or the Policies and Processes) will be available for audit.

7.5. Supporting Material

- Legal and Other Compliance Policy
- Legal, Regulatory and Contractual Requirements Registers.
- Compliance Reviews, Status Assessment and Audit Programmes,
- Legal, Regulatory and Standards – Externally sourced documents
08 How Telstra Global Manages, Measures and Improves

Telstra Global’s continual improvement model describes all stages of continual improvement. The stages include planning the security activities, creating programmes, agreeing performance levels, implementing the activities and checking their effectiveness through internal audit, monitoring performance, controlling non conformance, taking actions to correct or prevent failings and improving the effectiveness or efficiency of the management system.

In order for management to maintain visibility of Telstra Global’s performance and to ensure security continually meets requirements, recorded information and data is periodically reviewed and analysed. This information relates to aspects such as service performance and system audit activities.

Telstra Global views continual improvement as a crucially important and an essential activity. This is achieved by setting objectives, monitoring and measuring performance, and identifying areas of potential weakness from audit activities. Continual improvement is constantly reviewed by management and the need for it is communicated to all employees.

8.1. Policy and Process Ownership

Telstra Global has established a policy and process review programme. Each policy or process has a named owner who is responsible for ensuring that it remains fit for purpose.

The performance of selected policy or process is monitored, compliance verified and results are analysed along with other feedback from ISMS activities.
8.2. Risk Assessment

Telstra Global has established a risk assessment programme for all operational activities, information assets and resources. This process is described further in the How does Telstra Global manage information security risk section.

8.3. Training and Awareness

In order for employees to fulfil their roles and responsibilities, they must be competent to perform the tasks expected of them. Knowledge, skills and experience needs will be addressed by suitable education programmes and activities. Management judgement will be used to determine the most suitable educational format and content, together with the best source of education (internal, or external). Training levels and needs are tracked via a training needs analysis, reviewed as part of Telstra Global’s Management Review.

All employees and where relevant service providers are required to undertake a number of awareness training courses which are provided to them via an e-learning system that explains their responsibilities in accordance with Telstra Information Security and Business Continuity Policies and their contributions to the effectiveness of the ISMS and the consequences of non-compliance.

Additional training recommendations will be given to employees and where relevant service providers as deemed necessary as a result of risk assessment, incidents, and non-conformances.

A record of all training provided is maintained.

8.3.1. Supporting Material

- Human Resource Information Security Policy
- Training needs analysis,
- Training and awareness schedule / programme,
- Training and awareness materials (slides, documents, videos posters)
- Records of attendance, reviews of effectiveness

8.4. Compliance Audits

Telstra Global uses compliance audits to assess Telstra Global’s initiatives against its own and external standards. The external standards may be those of clients, independent third parties (e.g. information security consultants or other parts of the Telstra Corporation) or accredited certification bodies.

To ensure that the ISMS is effective, trained and competent employees will audit it and its associated policies and processes in accordance with an audit schedule.

The objectives for conducting compliance audits are:

- To determine if all the activities are being carried out in accordance to the defined policy or process.
- To ascertain the effectiveness of the ISMS in meeting customer agreed requirements and the objectives of the ISMS Policy.
- To determine if the policies, processes and controls can be further improved.

Auditors will undertake and report audits in line with the ISMS programme and present them at the Management Review meetings. Corrective actions and any resulting changes in processes and policy will be discussed and agreed.

8.4.1. Supporting Material

- Internal Audit Policy
- Internal Audit Schedule, Findings, Reports and Corrective Action log and plans
8.5. Information Security Incident Management

An information security incident or event is an identified occurrence of an operational, system, service or network state, indicating a possible breach of the Information Security Policy, or a failure of safeguards. Breaches of policy are investigated by the appointed members of the SIRT in accordance with the Incident Management Process, supported by relevant department head as appropriate.

As well as reporting incidents, employees and service providers are encouraged to report weaknesses in controls and safeguards so that preventive actions can be identified and implemented.

The Compliance and Standards Project Manager collates information about all such incidents, analyses trends and recommends the implementation of further controls if required.

8.5.1. Supporting Material

- Information Security Incidents Process
- Corrective Action Log
- Incident Reports
- Incident Analysis Report and Findings
- Recommended Actions

8.6. Performance Monitoring and Measurement

To focus the resources of the organisation and as part of the principle of continual improvement, management will agree and set targets for its ISMS activities at least annually. Using the GOSPA (Goals, Objectives, Strategies, Plans and Actions) Methodology, These shall be “SMART” targets i.e. specific, measurable, achievable, realistic and time-related and progress shall be monitored and measured as part of the review programme.

- The effectiveness of the policies / processes are monitored and performance measured
- The selected policy and process owners collect and analyse relevant data to determine how effective the processes are in achieving customer security requirements, set objectives and levels of performance improvement.

8.6.1. Supporting Material

- Performance Monitoring Process
- Performance objectives, KPIs and Targets (annual)
- Performance reports (quarterly or monthly)

8.7. Management Review

All the above ISMS activities will be subject to continual informal and periodic formal review, to best facilitate the goal of improvement. The purpose of the review itself is primarily to assess and decide, with the resulting decisions being communicated to relevant parties.

Management Reviews take place with the SMT to provide a means of maintaining clear visibility of all aspects of the business operation, and assessing the operational suitability and effectiveness of the complete Telstra Global ISMS.

The overall objectives of the reviews, (during which specific business issues are discussed and actions taken) are:

- To review the performance of Telstra Global over the previous period, from audits, incidents and service provider reviews.
• To ensure that all policies and processes are operating effectively and are adequate and sufficient to ensure compliance
• To determine where improvements can be made to further enhance operational capability
• To set objectives for the next period
• To assess the suitability of the Information Security Policy

Minutes of all Management Review meetings will be recorded and circulated with actions defined.

8.7.1. Supporting Material
• Management Review Policy
• Terms of Reference, Schedule and Minutes (decisions and agreed actions) of the various reviews
• Supporting reports submitted to the review

8.8. Continual Improvement (CA, PA, IA)

8.8.1. Corrective Actions
Corrective Action (CA): Appropriate action(s) to eliminate the cause of a non conformance or Non Compliance. Many various types of corrective actions exist including:

• Changing a set of access rights
• Fixing a software defect
• Revising a system configuration
• Revising a document
• Improving a process.

In the event that a product, process, service or management system non conformity is identified, Telstra Global will react by determining the root cause and initiating the appropriate corrective action.

Records will be maintained and the resolution of the problem monitored through to clearance of the non-conformity.

Failings in the ISMS shall be the subject of corrective action. In most cases, this will be captured on the corrective action log. However, wider failings may be the subject of a separate programme, or project.

8.8.2. Preventative Actions
Preventative Action (PA): Appropriate action(s) are undertaken to eliminate the causes of potential non conformity or non compliance in order to prevent their occurrence. Many various types of preventive actions are conducted such as:

• Management reviews
• The publication of corporate and local policies, processes & procedures
• Regular risk assessments on corporate information assets
• Undertaking risk assessments on the use of third parties and where applicable their connections to corporate assets
• Undertaking risk assessments on proposed new information systems
• Ensuring all employees are aware of information security, business continuity and legal issues
• Ensuring that all major information systems have monitoring activities in place for identifying potential abuse or attack

• Regular reviews of information security controls

• Regular testing and exercising of business continuity plans

• Ensuring that systems are updated with the latest security patches

• Ensuring that Antivirus systems are regularly updated

• Monitoring media sources for new threats and vulnerabilities.

The organisation favours the more proactive nature of carrying out preventative actions, based on data obtained from system and procedure audits, customer satisfaction, and the continuous reviewing of processes and methods.

Agreed preventative actions will be reviewed for their effectiveness in eliminating the root causes, thereby preventing reoccurrences.

8.8.3. Improvement Actions

Telstra Global is determined to ensure that actions needed to improve the effectiveness and efficiency of services or products are implemented as quickly as possible.

Appropriate action(s) to improve the efficiency and effectiveness of processes, procedures and activities are carried out within the ISMS. These include improvement actions that enable the ISMS activities to be faster, more cost effective and easier to deliver or undertake. Many various types of improvement actions are delivered such as:

• Simplifying ISMS processes and documents

• Automating processes

• Standardising processes across departments for consistency

• Implementing new methodologies / tools / skills

• Establishing small working groups to tackle special projects.

• Promotion of awareness training throughout the organisation

• Co-ordination of new initiatives.

8.8.4. Action review

Data from corrective, preventative and improvement actions will be presented at the Management Review.

8.8.5. Supporting Material

• Continual Improvement Action Management Policy

• Continual Improvement Action Register
09 Documented Information

The ISMS is supported by a comprehensive set of documented information.

9.1. Document Management

All documented information that forms part of the ISMS is subject to issue, approval and change control.

The following documents will be approved by the SMT and issued by the Compliance and Standards Project Manager:

- Information Security Policy
- This ISMS Framework
- Risk Assurance records, (including statement of applicability,asset identification, business impact analysis, control analysis and risk treatment plan).

All supporting policies, will be owned and approved by individual members of the SIRT as appropriate and issued by the Compliance and Standards Project Manager.

Processes, procedures, work instructions and forms will be owned and approved by individual members of the SIRT as appropriate and issued by the owner. Changes to ISMS documented information will be reviewed, authorised and published by the SIRT or individual Owners.

The master released copies of all ISMS documents are held electronically by the Compliance and Standards Project Manager, whilst local procedures, templates and checklists are held by their relevant owners, who will ensure that all appropriate documents are available and legible for the relevant users and will ensure that changes and current revision status of all ISMS documents are maintained.

Once a revision has been adopted and released, the previous version is archived into a separate area (accessible by the Compliance and Standards Project Manager or owner) for reference purposes only. When notified of revisions Employees and relevant third parties will be informed that any previous versions are obsolete and that hard or electronic copies should be disposed in accordance with their classification.

A register is maintained to log and track key ISMS documentation.
9.2. Record Management

Records provide evidence that an activity has taken place. They might be documents or information held in an electronic system. All documents that form part of the ISMS and support the provision of Telstra Global’s services and products will be clearly identified, controlled under appropriate change control and approved. Documentation also includes that which is created, stored transmitted and retrieved by electronic media. Their review, issue control, availability and distribution is all controlled. All records will be documented in the appropriate medium and retained for a suitable period. This may be anything from a formal document under change control, to an email.

Telstra Global will maintain a number documented policies, processes and key records. Where appropriate, they will be found in the Telstra Global EMEA DMS.

Information security records are identified along with retention periods within individual policies and processes.

9.3. Supporting Material

- Documented Information Policy
- Telstra ISMS Documents Register
010 Change History

<table>
<thead>
<tr>
<th>Issue number</th>
<th>Issue date</th>
<th>Details on the change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>29 June 2012</td>
<td>Initial Release</td>
</tr>
<tr>
<td>1.1</td>
<td>1st July 2013</td>
<td>Document Annual Review – Revised Headers, Footers and New Compliance section</td>
</tr>
<tr>
<td>2.0</td>
<td>1st October 2013</td>
<td>Alignment with ISO 27001:2013</td>
</tr>
</tbody>
</table>

Who to contact to if you have any queries, questions, changes or concerns.

<table>
<thead>
<tr>
<th>Document Owner</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>XXXX</td>
</tr>
<tr>
<td>Position:</td>
<td>COO EMEA, Operations &amp; Business Services</td>
</tr>
<tr>
<td>Email</td>
<td>XXXX</td>
</tr>
</tbody>
</table>