# Organization of information security

## Internal organization

*Axiom:* A structured management framework directs, monitors and controls the implementation of information security as a whole within <ORGANIZATION>

**NOTE: This is a generic structure chart (organogram). It should be replaced by one describing <ORGANIZATION>’s actual management structure for information security. All major components must be described below. The text that follows outlines a generic information security management structure based on ISO 27002 but this should be customized to suit <ORGANIZATION>’s specific management hierarchy, rôles and responsibilities.**

### Management commitment to information security

The **Board of Directors** **(“the Board”)** is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to the Executive Directors, led by the **Chief Executive Officer (CEO)**.

The **Executive Directors** give overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the **Security Committee (SC)** chaired by the **Chief Security Officer (CSO)**.

The Executive Directors depend heavily on the SC to coordinate activities throughout <ORGANIZATION>, ensuring that suitable policies are in place to support <ORGANIZATION>’s security principles and axioms. The Executive Directors also rely on feedback from the SC, CSO, ISM, auditors, Risk Management, Compliance, Legal and other functions to ensure that the principles, axioms and policies are being complied-with in practice.

The Executive Directors demonstrate their commitment to information security by:

* A statement of support from the CEO;
* Reviewing and re-approving the principles and axioms every year;
* Approving the IT budget including a specific element set aside for information security;
* Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests *etc*.

### Information security co-ordination

Information security activities should be co-ordinated throughout <ORGANIZATION> to ensure consistent application of the security principles, axioms and policy statements.

The Executive Directors have charged the SC with the task of securing <ORGANIZATION>’s assets. The SC is responsible for:

* Management oversight and direction for both physical and logical aspects of security, including information security;
* Coordinating and directing <ORGANIZATION>’s entire security framework, including the information security controls at all <ORGANIZATION> locations mediated through the Local Security Committees (see below) ;
* Commissioning or preparing information security policy statements, ensuring their compliance with the principles and axioms approved by the Executive Directors, and formally approving them for use throughout <ORGANIZATION>;
* Periodically reviewing the security policy statements to ensure the efficiency and effectiveness of the information security controls infrastructure as a whole, recommending improvements wherever necessary;
* Identifying significant trends and changes to <ORGANIZATION>’s information security risks and, where appropriate, proposing changes to the controls framework and/or policies for example by sponsoring major strategic initiatives to enhance information security;
* Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes;
* Periodically reporting on the status of the security controls infrastructure to the Executive Directors, and liaising as necessary with the Risk Management and Audit Committees *etc*., using metrics and other information supplied by the CSO, Local Security Committees, the ISM, Internal Audit and others.

The SC delegates some of its responsibilities (for example to the ISM, the Information Security function and Local Security Committees) but remains accountable to the Executive Directors for the overall effectiveness of information security throughout <ORGANIZATION>.

Business units or locations within <ORGANIZATION> have **Local Security Committees (LSCs)** which report to the SC. LSCs are responsible for:

* Providing the strategic direction, support and resources necessary to manage all types of local security issues and thus ensure that <ORGANIZATION>’s information assets are appropriately and consistently protected;
* Co‑ordinating and sharing information with each other to ensure consistent execution of the information security policy manual across all <ORGANIZATION> locations;
* Identifying specific **Significant Information Assets**, classifying them and nominating suitable **Information Asset Owners** (IAOs) for them;
* Gathering metrics and other information on the overall effectiveness of information security controls in their remit, and reporting this to the SC.

### Allocation of information security responsibilities

The Executive Directors have appointed a **Chief Security Officer (CSO)**. The **CSO** is responsible for:

* Chairing the SC;
* Taking the lead on information governance as a whole for example by issuing the policy manual and by providing the overall strategic direction, support and review necessary to ensure that information assets are identified and suitably protected throughout <ORGANIZATION>;
* Appointing and managing the ISM and Information Security Management team.

#### The **ISM** and **Information Security Management** are responsible for:

* Defining technical and non-technical information security standards, procedures and guidelines;
* Supporting IAOs and managers in the definition and implementation of controls, processes and supporting tools to comply with the policy manual and manage information security risks;
* Reviewing and monitoring compliance with the policy statements and contributing to Internal Audit and Control Self Assessment (CSA) processes;
* Collecting, analyzing and commenting on information security metrics and incidents;
* Supporting IAOs in the investigation and remediation of information security incidents or other policy violations;
* Liaising as necessary with related internal functions such as IT Operations, Risk Management, Compliance and Internal Audit, as well as the CSO, LSCs, SC and external functions such as the Police when appropriate;
* Organizing a security awareness campaign for personnel to enhance the security culture and develop a broad understanding of the requirements of ISO/IEC 27002.

#### **Managers** throughout <ORGANIZATION> are responsible for:

* Day-to-day implementation of the information security policy manual;
* Ensuring that suitable technical, physical and procedural controls are in place in accordance with the manual, and are properly applied and used by all workers. In particular, they should take measures to ensure that workers:
* Are informed of their obligations to fulfill relevant corporate policy statements by means of appropriate awareness, training and education activities;
* Comply with the policy statements and actively support the associated controls; and
* Are monitored to assess their compliance with the policy statements and the correct operation of the associated controls, and reminded of their obligations as appropriate;
* Providing the direction, resources, support, and review necessary to ensure that information assets are appropriately protected within their area of responsibility;
* Informing Information Security Management and/or IAOs of actual or suspected policy violations (information security incidents) affecting their assets; and
* Evaluating compliance with the policy axioms through the regular CSA process and occasional Internal Audits.

**Information Asset Owners** (IAOs) are managers held accountable for the protection of particular Significant Information Assets by their LSC or the SC. IAOs may delegate information security tasks to managers or other individuals but remain accountable for proper implementation of the tasks. IAOs are responsible for:

* Appropriate classification and protection of the information assets;
* Specifying and funding suitable protective controls;
* Authorizing access to information assets in accordance with the classification and business needs;
* [For new application system developments] Undertaking or commissioning information security risk assessments to ensure that the information security requirements are properly defined and documented during the early stages of development;
* Ensuring timely completion of regular system/data access reviews; and
* Monitoring compliance with protection requirements affecting their assets.

**All <ORGANIZATION> workers** (*i.e.* employees on the payroll and others acting in a similar capacity, such as contractors, consultants, student placements *etc*.) are responsible for complying with the principles, axioms and policies in the information security policy manual where relevant to their jobs. They are responsible for maintaining the security of all information entrusted to them. Upon hire, as a condition of employment, each worker undertakes to comply with <ORGANIZATION>’s information security policies. Any worker failing to comply with the security policies could be subject to disciplinary action, potentially including termination of employment or contract and/or prosecution.

**Exemptions process:** an IAO may propose exemptionsto principles, axioms or policy statements identified in the policy manual for an information asset under their remit. The ISM is responsible for analyzing risks arising from the proposed exemptions and, in most cases, specifying mitigating controls to minimize those risks. Proposed exemptions which the ISM considers could significantly impact <ORGANIZATION>’s information security risks may be referred up through the LSC, SC, CSO and/or the Executive Directors for approval, depending on the significance of the perceived risk. A programme (action plan) is normally required to ensure full compliance with the within a specified time frame, in other words exemptions are not indefinite. The IAO will be held accountable for the mitigating controls and the action plan, and must personally assume any additional risk relating to the policy exemption and the mitigating controls until the exemption is resolved.

Current exemptions must be reviewed at least annually by the SC, LSCs, CSO and ISM. In an annual status report to the Executive Directors, authorized exemptions must be listed, the reasons why policy exemptions exist must be clarified and plans to resolve the non-compliance with policy (typically by means of strategic investment to achieve compliance, or by modifying the policy) must be explained.

## Important note from IsecT Ltd.

 We have donated this short extract from our information security policy manual to [www.ISO27001security.com](http://www.ISO27001security.com) as a generic example ISMS document.

**This policy is unlikely to be entirely sufficient or suitable for you without customization**. This is a generic or model policy incorporating a selection of commonplace controls in this area. Because it is generic, it cannot fully reflect every user’s requirements. We are not familiar with your specific circumstances and cannot offer tailored guidance to suit your particular needs. It is not legal advice.

 This work is copyright © 2007, [ISO27k Forum](http://groups.google.com/group/iso27001security), some rights reserved. It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](http://creativecommons.org/licenses/by-nc-sa/3.0/). You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum at [www.ISO27001security.com](http://www.ISO27001security.com), and (c) if shared, derivative works are shared under the same terms as this.