



ISO/IEC 27001 & 27002 implementation guidance and metrics

Prepared by the international community of ISO27k implementers at ISO27001security.com

Version 1.1 19th November 2007

Introduction

This is a collaborative document created by ISO/IEC 27001 and 27002 implementers belonging to the [ISO27k implementers' forum](#). We wanted to document and share some pragmatic tips for implementing the information security management standards, plus potential metrics for measuring and reporting the status of information security, both referenced against the ISO/IEC standards.

Scope

This guidance covers all 39 control objectives listed in sections 5 through 15 of ISO/IEC 27002 plus, for completeness, the preceding section 4 on risk assessment and treatment.

Purpose

This document is meant to help others who are implementing or planning to implement the ISO/IEC information security management standards. Like the ISO/IEC standards, it is generic and needs to be tailored to your specific requirements.

Copyright



This work is copyright © 2007, [ISO27k implementers' forum](#), some rights reserved. It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](#). 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 implementers' forum (www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.

Ref.	Subject	Implementation tips	Potential metrics
4. Risk assessment and treatment			
4.1	Assessing security risks	Can use any information security risk management method, with a preference for documented, structured and generally accepted methods such as OCTAVE , MEHARI , ISO TR 13335 or BS 7799 Part 3 (and in due course ISO/IEC 27005).	Percentage of risks identified assessed as high, medium or low significance, plus 'un-assessed'.
4.2	Treating security risks	Management (specifically, the information asset owners) need to assess risks and decide what (if anything) to do about them. Such decisions must be documented as a Risk Treatment Plan (RTP). It is acceptable for management to decide explicitly to do nothing about certain information security risks deemed to be within the organization's "risk appetite", but not for this to be the default approach!	Trend in numbers of information security-related risks at each significance level. Information security costs as a Percentage of total revenue or IT budget. Percentage of information security risks for which satisfactory controls have been fully implemented.
5. Security policy			
5.1	Information security policy	Think in terms of an information security policy manual or wiki containing a coherent and internally consistent suite of policies, standards, procedures and guidelines. Identify review frequency of the information security policy and methods to disseminate it organization-wide. Review of suitability and adequacy of the information security policy may be included in management reviews.	Policy coverage (<i>i.e.</i> percentage of sections of ISO/IEC 27001/2 for which policies plus associated standards, procedures and guidelines have been specified, written, approved and issued). Extent of policy deployment and adoption across the organization (measured by Audit, management or Control Self Assessment).

Ref.	Subject	Implementation tips	Potential metrics
6. Organizing information security			
6.1	Internal organization	Mirror the structure and size of other specialist corporate functions such as Legal, Risk and Compliance.	<p>Percentage of organizational functions/business units for which a comprehensive strategy has been implemented to maintain information security risks within thresholds explicitly accepted by management.</p> <p>Percentage of employees who have (a) been assigned, and (b) formally accepted, information security rôles and responsibilities.</p>
6.2	External parties	<p>Inventory network connections and significant information flows to third parties, then risk assess them and review the information security controls in place against the requirements. This is bound to be scary, but it's 100% necessary!</p> <p>Consider requiring ISO/IEC 27001 certificates of critical business partners such as IT outsourcers, providers of security-related IT services <i>etc.</i></p>	Percentage of 3 rd -party connections that have been identified, risk-assessed and deemed secure.
7. Asset management			
7.1	Responsibility for assets	<p>Build and maintain an information asset registry (similar in nature to that prepared for Y2k), showing information asset owners (managers who are accountable for protecting their assets) and relevant asset details (e.g. locations, serial numbers, version numbers, dev/test/production status <i>etc.</i>).</p> <p>Use bar-codes to facilitate easy stock-takes/inventory checks and to associate IT equipment moving off- and on-site with employees.</p>	<p>Percentage of information assets at each stage of the classification process (identified / inventoried / asset owner nominated / risk assessed / classified / secured).</p> <p>Percentage of key information assets for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds</p>
7.2	Information classification	<p>Keep it simple! Aim to distinguish baseline (across-the-board) from enhanced security requirements according to risk.</p> <p>Start with confidentiality, perhaps, but don't neglect integrity and availability requirements.</p>	Percentage of information assets in each classification category (including not-yet-classified).

Ref.	Subject	Implementation tips	Potential metrics
8. Human resources security			
8.1	Prior to employment	In conjunction with HR, ensure a screening process is in-place that is commensurate with the security classification of the information to be accessed by the incoming employee. Simply put, the process of hiring should be a lot different for a clerk or an IT system administrator. Look into background checks, verification of claimed educational attainment and skill sets <i>etc.</i>	Percentage of new employees plus pseudo-employees (contractors, consultants, temps <i>etc.</i>) that have been fully screened and approved in accordance with company policies prior to starting work.
8.2	During employment	<p>Responsibility towards protection of information does not end when an employee leaves for home or leaves the organization. Ensure that this is clearly documented in awareness materials, employment contracts <i>etc.</i></p> <p>Consider an annual employment contract review by HR department with employees to refresh expectations stated in the terms and conditions of employment including their commitment to information security.</p>	Response to security awareness activities measured by, say, the number of emails and calls relating to individual awareness initiatives.
8.3	Termination or change of employment	<p>Refer to Section 7.1. Return of organization's assets when an employee leaves would be much easier to verify if your asset inventory was regularly updated and verified.</p> <p>Look at which accesses you need to revoke first when an employee files his/her resignation letter: which are the most critical or vulnerable systems?</p> <p>Track use of email by resignees prior to leaving in case they start sending confidential information out (subject to applicable policies and, perhaps, legal obligations re privacy).</p>	Percentage of userIDs belonging to people who have left the organization, separated into active (pending deactivation) and inactive (pending archival and deletion) categories.

Ref.	Subject	Implementation tips	Potential metrics
9. Physical and environmental security			
9.1	Secure areas	<p>The standard seems to focus on the computer suite but there are many other vulnerable areas to consider e.g. wiring closets, "departmental servers", and filing cabinets everywhere (remember: the standards are about securing information not just IT).</p> <p>Look into the ingress and egress of people into and from your organization. How far could the pizza or FedEx delivery person go without being challenged, authenticated and accompanied? What could they see or pick-up or hear while they are inside? Some organizations use color-coded identification tags to signify accessible areas by visitors. (e.g. Blue for 1st floor, Green for 3rd floor etc...). Now if you see a green ID on the 4th level, frag 'em!</p> <p>Be sure to retrieve staff and visitor passes when they leave. Have card-access systems disallow and alarm on attempted access. Have visitor passes turn opaque or otherwise appear invalid after so many hours from issue.</p>	<p>Reports from periodic physical security site surveys, including regular status updates on corrective items identified in previous surveys and still outstanding.</p>
9.2	Equipment security	<p>Have site security stop anyone (employees, visitors, IT support people, couriers and office removals people etc.) from removing IT equipment from site without written authority. Make this a visible deterrent with random stop-checks (if not airport-style metal detectors!). Be especially vigilant at back doors, loading ramps, smoking exits etc. Consider bar-coding equipment to make stop-checks and stock-checks more efficient.</p>	<p>Number of stop- or stock-checks performed in the previous month, and percentage of checks that revealed unauthorized movement of IT equipment, media etc. or other security issues.</p>

Ref.	Subject	Implementation tips	Potential metrics
10. Communications and operations management			
10.1	Operational procedures and responsibilities	Document information security procedures, standards and guidelines, plus roles and responsibilities, identified in the organization's information security policy manual.	Security-related IT process maturity metrics such as the "half-life" for applying security patches (the time taken to update at least half the population of vulnerable systems - this measure helps avoid the variable tail caused by the inevitable few systems that remain unpatched because they are not in daily use, are normally out of the office or whatever).
10.2	Third party service delivery management	Are you getting your money's worth? Answer this question and support it with facts by establishing a monitoring system for 3 rd -party service providers and their respective service deliveries. Look at periodic of review of service-level agreements (SLA) and compare it with monitoring records. A reward and penalty system may work in some cases. Watch out for changes that impact security.	<p>Cost of downtime due to non-fulfillment of service level agreements</p> <p>Performance evaluation of 3rd-party providers to include quality of service, delivery, cost <i>etc.</i></p>
10.3	System planning and acceptance	<p>Adopt structured processes for IT capacity planning, secure development, security testing <i>etc.</i>, using accepted standards such as ISO 20000 (ITIL) wherever possible.</p> <p>Define and mandate baseline (minimal acceptable) security standards for all operating system platforms, using security advice from CIS, NIST, NSA and operating system vendors and of course your own information security policies.</p>	<p>Percentage of emergency, high, medium and low risk changes.</p> <p>Numbers and trends of rolled-back/reversed-out changes, rejected changes vs. successful changes.</p> <p>Percentage of systems that (a) are supposed to comply with defined baseline security or similar technical security standards; and (b) have been proven by benchmarking/testing to comply fully with those standards.</p>
10.4	Protection against malicious and mobile code	Combine technological controls (<i>e.g.</i> anti-virus software) with non-technical measures (education, awareness and training). It is not much help having top of the line anti-virus software if employees keep on opening emails from unknown senders or downloading files from untrusted sites!	<p>Trends in the number of viruses, worms, Trojans or spams detected and stopped.</p> <p>Number and cumulative costs of malware incidents.</p>

Ref.	Subject	Implementation tips	Potential metrics
10.5	Back-up	<p>Implement back-up and restore procedures that satisfy not only contractual requirements but also the "internal" business requirements of the organization. Take inputs from the Risk Assessment exercise on what information assets are more significant and use this information in creating your back-up and restore strategy. Choice of storage, media to be used, back-up appliance, frequency of back-up and testing of back-up media needs to be decided upon and established.</p> <p>Encrypt backups and archives containing sensitive or valuable data (in practice, that's virtually all of them, otherwise why take backups?).</p>	<p>Percentage of back-up operations that are successful.</p> <p>Percentage of test backup restores that are successful.</p> <p>Mean travel time to retrieve back-up media from off-site storage to a successful restored state at all primary locations.</p> <p>Percentage of backups and archives containing sensitive or valuable data that are encrypted.</p>
10.6	Network security management	<p>Prepare and implement technical security standards, guidelines and procedures for network platforms and network security tools such as IDS/IPS, vulnerability management <i>etc.</i></p>	<p>Number of network security incidents identified in the previous month, divided into minor/significant/serious categories, with trends analysis and narrative descriptions of all serious incidents and adverse trends.</p>
10.7	Media handling	<p>Secure media and information in transit not only physically but also electronically (<i>via</i> the networks).</p> <p>Encrypt all sensitive/valuable data prior to being moved.</p>	<p>Percentage of physical backup/archive media that are fully encrypted.</p>
10.8	Exchange of information	<p>Look into alternate and "pre-approved" communications channels particularly secondary email addresses should the primary email address or mail server fail, and offline communications in case the networks are down. Verifying alternate comms channels would reduce stress in an actual incident.</p>	<p>Percentage of 3rd-party links for which information security requirements have been satisfactorily (a) defined and (b) implemented.</p>
10.9	Electronic commerce services	<p>Work closely with the business functions to develop secure eBusiness, by incorporating information security requirements into the projects and hence eCommerce systems from the outset (also any changes/upgrades thereafter). Emphasize the added value of security in reducing the commercial, legal and operational risks involved in entering into online business. Work on all three core aspects of security <i>i.e.</i> confidentiality, integrity and availability.</p>	<p>"eSecurity status" <i>i.e.</i> informed commentary on the overall management confidence level, based on analysis of recent penetration tests, current/recent incidents, current known vulnerabilities, planned changes <i>etc.</i></p>

Ref.	Subject	Implementation tips	Potential metrics
10.10	Monitoring	<p>The old quality assurance axiom "you can't control what you can't measure or monitor", holds true for information security. The necessity of implementing monitoring processes is now more evident as measurement of the effectiveness of controls is made an explicit requirement. Look at the criticality and significance of data that you are going to monitor and how this affects the overall business objectives of the organization in relation to information security.</p>	<p>Percentage of systems whose security logs are (a) appropriately configured, (b) securely captured to a centralised log management facility and (c) routinely monitored/reviewed/assessed.</p> <p>Trends in the number of security log entries that have (a) been captured; (b) been analyzed; and (c) led to follow-up activities.</p>
11. Access control			
11.1	Business requirement for access control	<p>Information asset owners who are held accountable by management for protecting "their" assets should have the ability to define and/or approve the access control rules and other information security controls. Make sure they are held to account for breaches, non-compliances and other incidents.</p>	<p>Percentage of corporate application systems for which suitable "owners" have (a) been identified, (b) formally accepted their ownership responsibilities, (c) undertaken (or commissioned) risk-based application security and access reviews, and (d) defined rôle-based access control rules.</p>
11.2	User access management	<p>Set up a discrete "security admin" function with operational responsibilities for applying the access control rules defined by application owners and Information Security Management.</p> <p>Invest in providing security admin with the tools to do their jobs as efficiently as possible.</p>	<p>Average delay between access change requests being raised and actioned, and number of access change requests actioned in the previous month (with trends analysis and commentary on any peaks/troughs e.g. "New Finance application implemented this month"...).</p>
11.3	User responsibilities	<p>Ensure security responsibilities are established and understood by the incumbent personnel. A good strategy is to clearly define and document responsibilities for information security in job descriptions or job profiles. Periodic review is a must to keep track of changes. Disseminate job profiles periodically to the employees (e.g. at annual performance appraisal time) to remind them of their responsibilities and gather any updates.</p>	<p>Percentage of job descriptions that include (a) fully documented and (b) formally accepted, information security responsibilities.</p>

Ref.	Subject	Implementation tips	Potential metrics
11.4	Network access control	Balance network perimeter (LAN/WAN) and internal (LAN/LAN) security controls against application security controls (defense in depth).	Firewall statistics such as percentage of outbound packets or sessions that are blocked (e.g. attempted access to blacklisted websites; number of potential hacking attacks repelled, categorized into trivial/of some concern/critical).
11.5	Operating system access control	Implement baseline security standards for all the main computing and telecoms platforms, reflecting best practice advice from CIS , NIST , system vendors <i>etc.</i>	System and network vulnerability statistics such as the number of known vulnerabilities closed, open and new; average speed of patching vulnerabilities (analyzed by vendor or in-house priorities/categories).
11.6	Application and information access control	Implement baseline security standards for all the main application systems and middleware, reflecting best practice advice and checklists from CIS , NIST , software vendors <i>etc.</i>	Percentage of platforms that are fully compliant with baseline security standards (as determined by independent testing), with notes on non-compliant systems (e.g. "Finance system due to be upgraded to compliant platform in Q4").
11.7	Mobile computing and teleworking	<p>Have clearly defined policies for the protection of not only mobile computing facilities themselves (<i>i.e.</i> laptops, PDAs <i>etc.</i>) but more importantly the information stored on them. As a rule, the information value far exceeds that of the hardware.</p> <p>Ensure the level of protection of information processing facilities being used inside the organization's premises "matches" the level of protection of your mobile computing facilities such as anti-virus software, patches, fixes, firewall software <i>etc.</i></p>	<p>"Mobile/teleworking security status" <i>i.e.</i> informed commentary on the current security status of mobile IT (laptops, PDAs, cellphones <i>etc.</i>) and teleworkers (home working, mobile workforce <i>etc.</i>), with notes on recent/current incidents, current known security vulnerabilities and projections of any increasing risks, coverage of defined secure configurations, antivirus, personal firewalls <i>etc.</i></p>

Ref.	Subject	Implementation tips	Potential metrics
12. Information systems acquisition, development and maintenance			
12.1	Security requirements of information systems	<p>Get "information asset owners" involved in high-level risk assessments and get their sign-off on security requirements arising. If they are truly accountable for protecting their assets, it is in their interest to get it right!</p> <p>Keep track of news on common or current vulnerabilities in applications and identify and implement appropriate protective or defensive measures. Implementation guidance can be obtained from several references, for example OWASP.</p>	See 11.1
12.2	Correct processing in applications	<p>Use standard libraries and functions wherever possible for common requirements such as data entry validation, range and type constraints, referential integrity <i>etc.</i></p> <p>Build and incorporate additional validation and cross-checking functions for greater confidence with vital data (<i>e.g.</i> control totals).</p> <p>Build and use automated and manual testing facilities and competencies to check for common issues such as buffer overflows, SQL injection <i>etc.</i></p>	Percentage of systems for which data validation controls have been adequately (a) defined; and (b) implemented and proven effective by thorough testing.
12.3	Cryptographic controls	<p>Use current formal standards such as AES rather than home-grown algorithms.</p> <p>Implementation is crucial!</p>	Percentage of systems containing valuable/sensitive data for which suitable cryptographic controls have been fully implemented (3- to 12-monthly reporting period).
12.4	Security of system files	Apply baseline security standards consistently, ensuring that best practice advice from CIS , NIST , system vendors <i>etc.</i> is followed.	Percentage of systems independently assessed as fully compliant with approved baseline security standards <i>vs.</i> those that have not been assessed, are not compliant, or for which no approved baseline exists.
12.5	Security in development and support processes	Embed information security into the system development lifecycle at all stages from conception to death of a system, by including security "hooks" in development and operations/change management procedures and methods.	"Developing systems security status" <i>i.e.</i> informed commentary on the current security status of the software development processes, with notes on recent/current incidents, current known security vulnerabilities and

Ref.	Subject	Implementation tips	Potential metrics
		Treat software development and implementation as a change process. Integrate security improvements into change management activities (e.g. procedural documentation and training for users and administrators).	projections of any increasing risks <i>etc.</i>
12.6	Technical vulnerability management	Track security patches constantly using vulnerability management and/or automated update tools where available (e.g. Microsoft Update or Secunia Software Inspector). Assess the relevance and criticality/urgency of patches in YOUR technical environment. Test and apply critical patches, or take other remedial actions, as quickly and as widely as possible for security vulnerabilities that affect your systems and are being actively exploited in the wild. Avoid falling so far behind on the version update treadmill that your systems fall out of support.	Patch latency <i>i.e.</i> deployment half-life (time taken to patch half the vulnerable population of systems - avoids seemingly random changes due to a few very late systems such as portables out in the field or in store).
13. Information security incident management			
13.1	Reporting information security events and weaknesses	Set up and publicise a hotline (generally the standard IT Help/Service Desk) for people to report security-related incidents, near misses and concerns.	IT Help/Service Desk statistics with some analysis of the number and types of calls relating to information security (e.g. password changes; queries about information security risks and controls as a Percentage of all queries). From the stats, create and publish a league table of departments (adjusted for number of employees per dept), showing those that are clearly security-conscious vs. those that are evidently asleep at the wheel.
13.2	Management of information security incidents and improvements	Post-incident reviews and case studies on serious incidents such as frauds illustrate control weaknesses, identify improvement opportunities and also form an effective security awareness-raising mechanism in themselves.	Number and gravity of breaches, if not some assessment of their costs to analyze, stop and repair the breaches and any tangible and intangible losses incurred. Percentage of security incidents that caused costs above acceptable thresholds defined by management.

Ref.	Subject	Implementation tips	Potential metrics
14. Business continuity management			
14.1	Information security aspects of business continuity management	<p>Treat business continuity management as a "management" process with inputs coming from various functions (top management, IT, operations, HR <i>etc.</i>) and activities (risk assessment <i>etc.</i>).</p> <p>Ensure consistency and awareness by relevant people and organizational units in the business continuity plans.</p> <p>Relevant exercises (such as desktop testing, simulation, full failover testing <i>etc.</i>) should be conducted (a) to keep the plans updated, (b) to improve management confidence in the plans, and (c) to make relevant employees familiar with their roles and responsibilities under disaster conditions.</p> <p>Get implementation guidance from BS 25999 - Business Continuity Management.</p>	<p>Percentage of business continuity plans at each stage of the lifecycle (needed / specified / documented / proven).</p> <p>Percentage of organizational units with business continuity plans that have been adequately (a) documented and (b) proven by suitable testing within the past 12 months.</p>
15. Compliance			
15.1	Compliance with legal requirements	Get qualified legal advice, especially if the organization operates or has customers in multiple jurisdictions.	<p>Number of legal compliance issues or recommendations grouped and analyzed by status (closed, open, new, overdue) and significance or risk level (high, medium or low).</p> <p>Percentage of key external requirements with which the organization has been deemed by objective audit or other acceptable means to be in compliance.</p>
15.2	Compliance with security policies and standards and technical compliance	Align security controls self assessment processes with self assessments for corporate governance, legal/regulatory compliance <i>etc.</i> , supplemented by management reviews and independent sanity checks.	<p>Number of internal policy and other compliance issues or recommendations grouped and analyzed by status (closed, open, new, overdue) and significance or risk level (high, medium or low).</p> <p>Percentage of information security compliance reviews with no substantial violations noted.</p>

Ref.	Subject	Implementation tips	Potential metrics
15.3	Information systems audit considerations	<p>Invest in a qualified IT audit function that uses the ISO27k, COBIT, ITIL, CMM and similar best practice standards/methods as benchmarks for comparison.</p> <p>Look into ISO 19011 Guidelines for quality and/or environmental management systems auditing as a valuable source for the conduct of internal ISMS audits. ISO 19011 provides an excellent framework for creating an internal audit programme and also contains qualifications of the internal audit team.</p>	<p>Number of audit issues or recommendations grouped and analyzed by status (closed, open, new, overdue) and significance or risk level (high, medium or low).</p> <p>Percentage of information security-related audit findings that have been resolved and closed vs. those opened in the same period.</p> <p>Mean actual resolution/closure time for recommendations relative to the dates agreed by management on completion of audits</p>

*** End of table ***

References to additional sources of information

Berinato, S. (2005). "[A Few Good Metrics](#)". CSO Magazine, July. Focuses on selecting and measuring a few useful metrics rather than a large number of useless ones. Creative presentation ideas for management reports.

Berinato, S., Campbell, G., Mena, C., and Lefler, D. (2005). "[Influencing Senior Management - Security Metrics](#)". Presentation to CSO Executive Council. Advice on the selection of S.M.A.R.T. security metrics that are few in number, up-to-date and accurate, validated and approved by stakeholders, and (above all) useful.

Hinson, G. (2006). "[7 Myths About Security Metrics](#)". ISSA Journal, July. Discusses design considerations for a security metrics system, with a few examples.

Hauser, J.R. and Katz, G.M. (1998). "[Metrics: You Are What You Measure](#)". MIT. A thought -provoking paper that warns about the dangers of driving a process in an unintended direction through the use of inappropriate metrics.

[ISO/IEC 27001:2005](#). "International standard - Information technology - Security techniques - Information security management systems - Requirements."

[ISO/IEC 27002:2005](#). "International standard - Information technology - Security techniques - Code of practice for information security management." [formerly known as ISO/IEC 17799:2005]

NIST (National Institute of Standards and Technology) (2003). "[Security Metrics Guide for Information Technology Systems](#)". Special Publication 800-55. Includes an extraordinarily comprehensive list of possible metrics (but unfortunately not much help on how to select *useful* metrics!). The first public draft of Special Publication 800-80 "[Guide for Developing Performance Metrics for Information Security](#)" is open for comment. NIST has [many more security standards](#).

Change record

Version 1.1 November 19th 2007

Corrected typos and broken/missing links discovered when this document was translated into Spanish (thanks [Javier](#) :-).

Version 1 June 28th 2007

Published by the [ISO27k implementers' forum](#). Contributions from Gary Hinson, H Deura, K, Ramiah Marappan, Rainier Vergara and Richard O. Regalado.

Feedback

Comments, queries and improvement suggestions (especially improvement suggestions!) are welcome either via the [ISO27k implementers' forum](#) or direct to the forum administrator Gary@isect.com