CyTRAP Labs and ARRAY Development

Roentgenstrasse 49 Street
CH-8005 Zuerich Zip Code
Switzerland Country

+41(0)44 272 1876 Voice
+41(0)76 200 7778 Cell

regustand.CyTRAP.eu URL
Urs+Nahum-Checklist CYTRAP.eu Email

Urs E. Gattiker, CyTRAP Labs, Zuerich, Switzerland

Nahum Goldmann, ARRAY Development, Ottawa, Canada

Urs+Nahum's Security Checklist

A comprehensive rated checklist of comparative security metrics for Small and Medium Enterprises (SMEs)

ISBN: 978-0-9783768-0-2

Version: 2007-05-18

DOWNLOAD

Get the latest version as well as updates from: **http://ReguStand.CyTRAP.eu/?p=1**

BIBLIOGRAPHIC REFERENCE

> Gattiker, Urs E. and Goldmann, Nahum – *Urs+Nahum's Security Checklist [online]. A comprehensive rated checklist of comparative security metrics for Small and Medium Enterprises (SMEs).*– Published in Zurich & Lethbridge (Alberta) by CyTRAP Labs -- Access: <*http://ReguStand.CyTRAP.eu/?p=1*> ISBN 978-0-9783768-0-2

Abstract

A Comprehensive Rated Checklist of Comparative Security Metrics for better IT Governance in Small and Medium Enterprise (SME), in particular Financial Institutions.

This checklist was developed by Urs E. Gattiker, Nahum Goldmann and their colleagues at CyTRAP Labs, experts in risk management and legal compliance for their clients.

The checklist is founded in our belief that comprehensive compliance and risk management systems are a key defense against significant losses, violations, customer harm and ultimately, the failure of a firm. Failure to comply may result in legal consequences for c-level executives and members of the board of directors besides being fined and having to deal with litigation.

Our checklist provides the enterprise with a systematic framework to better manage the firm's compliance efforts and activities designed to reduce the various risks. You may provide this list to your IT personnel. They will have to spend 10-20 days to scan and do a cursory first read of the materials that form the basis of this checklist.

If you have comments or questions or would like to discuss issues regarding this checklist and its use in your enterprise, we would appreciate hearing from you.

Contact:

Urs E. Gattiker, (see contacts and bio at *http://info.cytrap.eu/?page_id=2*):

Email: Urs+Nahum-Checklist at CYTRAP.eu

Phone: +41 (0)44 272-1876 or +41 (0)76 200 77 78

Table of Contents

Introduction

This Checklist covers common IT security laws, standards, regulations and best practices that are necessary for an enterprise to establish a baseline level of security, expose high risk areas, safeguard confidentiality, protect information assets and intellectual property, and ensure legal compliance.

Keeping Critical Information Safe and Secure

Every organization must implement the following five principal steps to keep its critical information safe and secure:

1. **Put in place and enforce policies that follow best security and risk-management practices**
   - Devise holistic corporate security and risk-management strategies.
   - Develop company policies that help maintain confidentiality, control, integrity, authenticity, availability and utility of business information.
   - Implement sound business practices, regulatory enforcement and technical tools to reduce the risk of security breaches and fraud.
   - Ensure corporate executive accountability, regulatory compliance and effective internal controls.
   - Provide management with security metrics and vulnerability-assessment information about critical processes and operations.
2. **Properly configure information assets and minimize attacks from internal and external sources**
   - Document system, hardware and software configurations.
   - Plan, configure and monitor defenses of your system against internal and external threats.
   - Minimize the likelihood of exploitation of threats and vulnerabilities.
   - Prepare for contingencies.
3. **Catalog, classify and dispose data properly**
   - Know what personal and business information has been collected.
   - Keep data locked for all unauthorized persons.
   - If you no longer need business data, move them to a safe archive.
   - Delete unnecessary information properly at the appropriate time.
   - Eliminate unneeded data and dispose of them securely (e.g., wipe and dispose them from hard drives and USB-sticks using data destruction methods, thus guaranteeing appropriate degrees of unrecoverability).
4. **Provide critical incident response, alarms and continuity management**
   - Have tried and tested plans for responding to a range of security incidents.

- Assure business continuity for critical functions and provide paths for resumption of normal operations.

5. **Conduct periodic internal and external audits and assessments**
    - Conduct regular internal security audits to verify compliance with established security policies and procedures.
    - Evaluate and act upon prioritized recommendations from internal auditors, ensuring compliance with fiduciary responsibilities for safeguarding personally-identifiable information and corporate assets
    - Ensure management accountability and compliance with regulatory agency requirements, by taking periodic external, independent and impartial audits and assessments of current IT security and risk-management policies, procedures and practices.
    - Ensure corporate compliance with state regulation, baselines, standards, codes and industry requirements.
    - Disclose the results of external audits and assessments to the principal stakeholders, such as customers, investors, executives, government inspectors and auditors, in a transparent and timely manner.

To effectively implement the above steps, an Small and Medium Enterprise (SME) has to systematically assess business processes and address the types of risks to which the corporate data might be exposed. This process is often challenging even for a large multinational or government organization with vast resources. Overwhelmed by numerous, sometime conflicting, and often costly IT security requirements advanced by various governments, regulatory authorities and industry associations, a typical SME might decide that its best strategy is to ignore all of them, imagining that only large organizations are vulnerable.

Use of the Checklist

This document provides an easy-to-understand checklist for SMEs that allows them to intelligently navigate the ocean of defensive security measures. To ensure consideration of the worst case scenario, we have emphasized the requirements for small Financial Institutions (FIs) as a subset of SMEs. FIs are typically heavily regulated and provide the most attractive target for various villains ("*because that's where the money is*"). This Checklist is also applicable to all small, medium and even large organizations, whether in industry, government, or non-profit.

The Checklist provides corporate executives, as well as financial and technical management and personnel, with a pragmatic map for action; i.e., it offers a rated list of practical security procedures to ensure corporate IT defenses, to ascertain the internal controls and to facilitate the corporate board’s assessment of potential IT security threats affecting strategic objectives. Documenting and auditing IT security procedures and reporting findings to the shareholders and regulators is typically required by business accountability legislation, such as Sarbanes-Oxley Act (USA), Realignment of the Swiss CO – Art 727 CO: (Art 728a Para 1 Nr. 3 CO), or KonTrag (Germany).

'Pragmatic' means here that our Chart is regretfully not for the use by the companies that need it most, as the executives whose IT systems have really bad security problems are typically in the denial, and hence cannot be helped. Rather it would be most helpful to these executives that are already fully committed to security and that would implement security solutions anyway; it is just that by using the Chart they might make security implementation faster, easier and less expensive.

The action items listed in the checklist are based mainly on a about a dozen comprehensive laws, standards and regulations published by internationally-recognized regulatory bodies, as well as on the top security guides, handbooks and critical publications on the subject. The key hallenge that we have faced was how to integrate all these documents in a consistent way that would ensure that we do not duplicate essentially similar-action clauses integrated from various documents.

Our Checklist is hardly a legal document, as it typically just refers its users to the appropriate regulatory sources. It is intended to help financial SMEs and other organizations to achieve best practices for securing and safeguarding strategically important assets, data and information.

Our principal goal was to consolidate variations on essentially the same defensive or risk avoidance actions by amalgamating the fundamentals of specific recommendations or requirements from various documents cited, even if there were discrepancies or minor contradictions among the variants. We also selected only those sources that would be sufficient for most regulatory requirements while helping the user to manage risks most effectively.

The Checklist is not intended to impose a specific model or theoretical construct on its users; indeed, its practical orientation is in our opinion a strength for the SME industry segment.

Multinational Enterprises

Multinational enterprises, even SMEs, must consider that local regulations usually take precedent over the corporate ones or over the legislation of the country where corporate headquarters are located. Nonetheless, the company might have to comply with all of them (e.g., the Sarbanes-Oxley Act or the Patriot Act for the overseas divisions of the US companies). Moreover, while a directive, e.g., a privacy directive in the European Union, might be implemented slightly differently across the 27 Member States, a regulation must be implemented by each Member State exactly as stated, without considering national peculiarities.

Globalization is making regulatory compliance ever more complex. For instance, a Swiss Holding company might have to comply with the Realignment of the Swiss CO – Art 727 CO: (Art 728a Para 1 Nr. 3 CO) and, due to its international activities, also with the European Union regulations, Sarbanes-Oxley Act and so on. We have structured the checklist to respond to this reality by using security guides and handbooks that apply to more than one jurisdiction.

For instance, unless an enterprise is absolutely certain that it has no personal data (e.g., mailing address, social security number, bank account information) stored anywhere on any device about a U.S. customer, data-security breach legislation, such as California's SB-1386, must be considered carefully to avoid expensive litigation down the road. The checklist encourages that approach by looking beyond the obvious while providing managers with the support needed to manage these risks and get the necessary process changes in place quickly and efficiently.

A first assessment will undoubtedly reveal certain shortcomings and the areas where the current security situation would not meet the expected organizational quality standards. We recommend involving independent and impartial external auditors as early as possible in addition to the internal ones. Joint objective assessment of the state of organizational security could be conducted by going through the whole checklist in order from the most severe to the lowest risks.

Security is not a one-point shot with a silver bullet but a continuous process whereby the organization has to constantly strive for improvement. In most countries, annual assessment of IT security efforts by external auditors is becoming the rule. Implemented security measures must satisfy auditors to issue a clean bill of health that will become a part of the shareholder report.

Checklist Compliance Rating

Compliance Risk Assessment

*****	**Severe**	The lowest hanging fruits, cheapest and easiest to implement upfront, or when absolutely no waiting is allowed (i.e., if legal compliance is required)
****	**Critical**	Less easy to implement, but still short term priorities
***	**Essential**	As essential as the higher ratings, but realistically slower or more expensive to implement
**	**Recommended**	Should be considered, especially if the resources allowed and the higher ratings have already been implemented
*	**Low**	Nice to have if resources permit

Our star rating should provide a convenient path to achieving and maintaining security over an extended time period, particularly for an organization of limited resources. In line with typical SME concerns, it is biased towards the urgency and feasability of implementation. SME executives must understand that it is critical first to implement all the 5-star measures, than the 4-stars, and so on. Ideally, users will consider implementation of all the clauses of 3 stars and higher from our Checklist.

Our star rating is not intended to rate the *importance* of the clauses in the Checklist. Counter-intuitive as it might be to any reasonable person who is not a security expert, they are all equally important. This is because overall security of a given system is only as good as its weakest link. Often, neglecting an esoteric, an unlikely—to—be-compromised, a seemingly minor, or a fairly routine security measure helps a determined penetrator to take over an otherwise secure system.

The only exception to the equality of all organizational security measures is anything that relates to policy development and structuring the procedures, as these activities are usually more important than others. In general, it is unwise to try developing comprehensive security defenses without an overall corporate vision; however an SME that has not yet developed such a vision should not delay all security improvements until its security policy and action plan are in place. There are many actions that a company can and should implement right away regardless whether it already has approved the comprehensive and holistic security-implementation plan.

Thus, although it is critically important to develop a good overall security plan and policy, using our checklist rating, it would only merit 4 out of 5, as typically there are much lower-hanging fruits around, such as preventing exploits that can be used at once. Similarly, ensuring accountability by taking periodic external, independent and impartial audits of current IT security and risk management efforts is critical for corporate survival. However, such comprehensive measures require preparation and cannot realistically be implemented overnight[1].

In summary, the need for a comprehensive security policy should not prevent immediate implementation of obvious and critical security improvements such as placing high-quality locks placed on the server room doors, ensuring periodic updates of the operating systems, and installing anti-virus protection on workstations.

Still, it is really up to the executive to decide what is the road to the most effective and speedy implementation, taking into account that SMEs often operate in the survival mode and can allocate to security only so much time and resources. To be on the safe side, always consider security implementation as a life-long journey, with more stars assigned to more urgent steps.

Using the Checklist and addressing high-star risks, corporate management should be able to provide effective security oversight improve organizational security in pragmatic and cost-effective ways.

Finally, personnel must be encouraged to report all security and risk problems they encounter or perceive without the fear of retaliation for doing so. Corporate culture plays a crucial role in encouraging an atmosphere of collaboration for better security.

[1] Nonetheless, a prudent executive should aim to conduct security audits as soon as possible, even before all possible security measures have been implemented. Initial internal and external audits can be useful to establish quantitative benchmarks and clarify executive accountabilities; subsequent audits should be used to check on progress in meeting commitments and to correct implementation flaws. Note that corporate IT and security departments sometimes postpone audits indefinitely, perhaps in an unconscious (or even conscious) attempt to avoid accountability for inadequate performance. *When* (not *if*) the inevitable disaster strikes, such managers may bolt from their jobs, leaving the remaining operational executives to sort out the mess. According to various postmortem studies, an average SME rarely survives a major online security breach for more than half a year. Hence, it is in the direct interest of its stakeholders to ensure that external audits indeed take place regularly.

The Checklist

Below we provide you with our checklist and ratings as described above.

Before starting with the checklist in detail we urge you to read the documents we cite further below (we provide you with the links you need to download the documents – laws, regulations for free). Please be aware that it will take several weeks time before your staff will have read all the materials and become familiar with them.

The checklist helps to conduct reviews, whereby assessors are looking for areas where the firm's controls are weak or inadequate. Subsequently, thorough reviews in those areas potential deficiencies and possible violations of laws and rules can be identified. Therefore, the first type of examination focuses on the structure and operation of a firm's risk management processes and systems. The second type of examination gives one the overview of how well a firm is self-policing its activities is the comprehensive compliance examination. This examination focuses on compliance with financial, data privacy, accounting and other pertinent laws and regulations.

You may provide this list to your IT personnel. We advice you that it will take them 10-20 days of getting themselves started reading the materials that are the basis of this checklist. If we can support you in these efforts please do not hesitate to contact us.

If you have questions, comments or need advice pertaining the the Security Checklist, we would appreciate having a chance to talk to you.

Urs E. Gattiker (see contacts and bio at http://info.cytrap.eu/?page_id=2):

Email: Urs+Nahum-Checklist at CYTRAP.eu

Phone: +41 (0)44 272-1876 or +41 (0)76 200 77 78

1. Laws, Regulations and Contracts

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
1.1	****	Conduct corporate board's review of the effectiveness of the group's system of internal controls and report the results to the stakeholders. The review should cover all material controls, including financial, operational and compliance, as well as risk-management systems.	Annually	The Combined Code on Corporate Governance; Sarbanes-Oxley Sec. 404. Management assessment of internal controls; Realignment of the Swiss CO – Art 727 CO: (Art 728a Para 1 Nr. 3 CO), ISO/IEC 17799:2005 Chapter 0.4, 0.5
1.2	****	Check whether meaningful information on the purposes for the collection and use or disclosure of personal data was given to each customer, and their consent was given for use or changed use from the original purpose for which the data were collected.	Annually	BSI – Chap 1; Guidelines regarding Internet and email surveillance at work, Chapter 5.2, 6;

1.3	***	Check whether the data protection officer has the authority and support to intervene on privacy issues in relation to all organizational operations.	Annually	BSI – Chap 1;
				Change in the Federal Data Protection Act 3.§ 4g.c) (2a);
				ISO/IEC 17799:2005 Chapter 6.1.3

1.4	***	Ensure that procedures regarding the personal transportation of data media and IT components are well-structured and compliance is monitored with spot-checks.	Annually	BSI – S 2.218; ISO/IEC 17799:2005 Chapter 9.2.5 11.7.1

		Operational		
1.5	****	Ensure that users' (e.g., suppliers, employees, customers) agreements on usage monitoring are up-to-date, to prevent and detect misuse of information.	Annually	ISO/IEC 17799:2005 – Chapter 15.1.5; Guidelines regarding Internet and email surveillance at work;
1.6	****	Check whether a formalized procedure to respond to a request for access to personal information within 30 days is operational and well documented.	Annually	BSI – Chap 1; Privacy; Your privacy responsibilities – Priv. Com Ontario
1.7	****	Check whether employee agreement and consent permits the archiving of private and corporate data (e.g., email)	Annually	BSI – Chap 1; Guidelines regarding Internet and email surveillance at work, Chapter 5.4

1.8	****	Check whether the firm has designated a data-protection officer (neither IT security nor sysadmin) to ensure data protection and privacy compliance (if no person assigned – outsourcing is possible; if none – responsibility falls back to CEO)	Quarterly	Change in the Federal Data Protection Act – Germany;
				BSI – Chap 1, S2.193, S4.78;
				ISO/IEC 17799:2005 Chapter 6.1.3

1.9	***	Check whether customers and employees can, if required, make use of complaint procedures that provide effective recourse for correcting information handling practices and policies.	Annually	BSI – Chap 1; Your privacy responsibilities; Guidelines regarding Internet and email surveillance at work, Chapter 6;
1.10	***	Check whether relevant administrative regulations, ordinances, and service regulations are adhered to, and whether pre-planning for changes is taking place due to amendments coming into effect in the next 36 months.	Annually	BSI – Chap 1, Gattiker, 2004;
1.11	***	Check whether rights to access a private device (e.g., a home workstation, notebook or mobile phone) from the work system have been secured from the employee, to ensure availability of files, data and synchronization of databases for telecommuting or mobile working; whether logging out after use is required; and compliance is being monitored.	Annually	BSI – S2.112, S3.18, T2; ISO/IEC 17799:2005 Chapter 11

1.12	***	Check whether information has been safeguarded and legally enforced from unauthorized access, disclosure, copying, use or modification.	Annually	California's S.B. 1386;
				BSI – Chap 1, S2.220;
				ISO/IEC 17799:2005 Chapter 11.4, 11.5, 11.6

1.13	***	Ensure that a contract with a vendor or outsourcer stipulates that the system will function according to contracted specification (i.e., the legal principle is 'reliance').	Annually	Gattiker (2006); ISO/IEC 17799:2005 Chapter 10.2.2
1.14	***	Before outsourcing or security services contracts are signed, check whether the wording potentially covering liability (*for what, when, etc.*) is clear, including specifying how data should be treated, employees hired (e.g., background checks and level of expertise) and supervised, thus ensuring that contract provisions (such as doing background checks on employees or adequately securing data) are being upheld.	Annually	BSI – 3.10; Gattiker (2006); ISO/IEC 17799:2005 Chapter 6.2.3., 10.5.5
1.15	***	Check whether security requirements for outsourcing projects are regularly updated and flow into contractual arrangements.	Annually	BSI – S 2.251, S2.253, S2.256; ISO/IEC 17799:2005 Chapter 6.2.3., 10.5.5
1.16	***	Check whether data-storage devices that are no longer needed are disposed of securely (e.g., recycling of equipment and disposing of hard drives and USB-sticks).	Semi-Annually	BSI – S4.200

2. Security Policies and Performance Metrics

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
2.1	****	Develop corporate security and risk management policies that help maintain confidentiality, integrity and availability of business information.	Annually	Gattiker, 2007
2.2	****	Establish Key Performance Indicators (KPIs) that help track corporate objectives regarding protecting the confidentiality, integrity and availability of information, as identified in the corporate strategy.	Semi-Annually	Gattiker, 2007; ISO/IEC 17799:2005 Chapter 6.1.1

2.3	***	Assess whether implementation metrics have been developed and implemented and are being monitored regarding serious violations of security policies (e.g., access policy, privacy policy).	Semi-Annually	ISO/IEC 17799:2005 Chapter 0.8;
				NIST – SP800-100 – Chapter 7;
				Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz – Chapter 8.4;

2.4	***	Check whether impact metrics address how certain outcomes (e.g., policy violations, data security breaches and lost mobile phones) affect or interrupt business operations; i.e. illustrate strategic links.	Semi-Annually	NIST – SP800-80 – Chapter 5; Sarbanes-Oxley 2002 – Section 404
2.5	****	Assess whether metrics have been developed and implemented and are being monitored regarding proper use of company equipment including access to the corporate LAN from a remote location (e.g., a public PC in a hotel lobby or a home computer).	Semi-Annually	BSI – Chap. 7.6; 4.200;
		Operational		

2.6	****	Ensure that the enterprise regularly reviews and analyzes audit records for indications of inappropriate or unusual activity, and takes information for remedial actions.	Semi-Annually	The Combined Code on Corporate Governance;
				ISO/IEC 17799:2005 Chapter 13.2;
				NIST – SP800-80 – Chapter 5;
				Goldmann & Orton, 2001;
				Sarbanes-Oxley 2002 – Section 404

#	Rat-ing	Actions	Frequency	Documents to Consult

2.7	***	Measure the absolute number of audit findings deviating from the acceptable norm.	Semi-Annually	COBIT 2.5, 4.7;
				NIST – SP800-80 – Chapter 5;
				Wagner & Gattiker, 2007

2.8	***	Ascertain that some types of automated or semi-automated mechanisms are being used to conduct audit analysis and report summary findings of inappropriate activities; and control whether implemented responses improve performance.	Semi-Annually	COBIT 2.5, 4.7
				ISO/IEC 17799:2005 Chapter 12.2;
				ISO/IEC 27001:2005 Annex A;
				NIST – SP800-80 – Chapter 5;
				Sarbanes-Oxley 2002 – Section 404

2.9	***	Estimate the percentage of critical security incidents caused by improperly configured access controls (requires integrating information from access control policy and procedures, incident monitoring, audit monitoring/analysis and monitoring configuration changes/patch latency).	Semi-Annually	Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz – Chapter 8.4;
				NIST – SP800-80 – Chapter 5;

3. Compliance and Risk Management

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		

3.1	****	Ensure accountability by taking periodic external, independent and impartial audits of current IT security and risk management efforts.	Annually	COBIT ME4 Monitor and Evaluate, COBIT 2.5, 4.7, Appendix III;
				Goldmann & Orton, Chapter 20;
				Sarbanes-Oxley 2002 – Section 404

3.2	****	Check whether the enterprise has a tried and tested business continuity and recovery plan in place.	Annually	BSI – S4.173, S6.11; EBIOS Sect. 5 – 3.2.9, 3.3.7

3.3	***	Review information security program to ensure legal compliance for today and tomorrow.	Annually	BSI – S 2.192;
				COBIT A15.2, AI5.2, 3.7;
				Sarbanes-Oxley 2002 – Section 404

3.4	***	Ascertain that there is a tried and tested critical incident response procedure in place in case of a security breach (e.g., a hacking attack or unauthorized access).	Semi-Annually	BSI – S2.158, S6.9;
				COBIT – Deliver and Support – DS8.3 Incident Escalation;
				ISO/IEC 17799:2005 Chapter 11.4, 11.5

		Operational		
3.5	*****	Regularly conduct a protocol-tracking analysis that includes penetration testing and, most important, assesses which devices communicate with each other, to ensure compliance with network policy (i.e. discover botnet activities, abnormal resource demands, or use of unauthorized software and rogue wireless routers and others).	Quarterly	Wagner & Gattiker, 2007; ISO/IEC 17799:2005 – Chapter 15.2.2 – Technical Compliance checking

3.6	*****	Monitor and inspect user logs as a part of the protocol-tracking analysis, to uncover unauthorized usage of software and browsing of dangerous or unsuitable web sites.	Monthly	Wagner & Gattiker, 2007;
				ISO/IEC 17799:2005 – Chapter 15.1.2, 15.1.4;

3.7	****	Transparently communicate risk and audit findings to the stakeholders (i.e., clients, investors, executives, government inspectors).	Annually	COBIT – PO6 Communicate Management Aims and Direction; Goldmann & Orton, 2002

#	Rat-ing	Actions	Frequency	Documents to Consult
3.8	***	Specify the organization's information systems while describing the assumptions and security rules, and identifying the constraints.	Annually	EBIOS Sect 2 – Activity Steps 1-2, Sect 3 – Techniques – Step 1; ISO/IEC 26300 – 12.2 Other Information

3.9	***	Check whether the building that houses the network meets all local building codes.	Annually	BSI – 4., 4.1–4.4, 4.6;
				EBIOS – Section 4 – PHY_LIE.2 premises;
				ISO/IEC 17799:2005 Chapter 9.1.2;
				ISO/IEC 26300 – Chapter 9.1.1

3.10	***	Check whether your business partners and service providers have security measures in place that meet compliance regulations your firm is subjected to.	Annually and when signing the Service Level Agreements	BSI – 3.10;
				COBIT DS1 – Define and Manage Service Levels;
				EBIOS – Section 5 – BOS_SOT.1.2

4. Human Resources

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
4.1	****	Assess whether appropriate resources have been committed to information security (i.e., money and human resources).	Semi-Annually	ISO/IEC 17799:2005 – Chapter 8
4.2	*****	Control that regular awareness-raising efforts make employees understand why certain behaviors violate policy and jeopardize confidentiality of data, such as: • Not allowing friends and family to use the company laptop, • Not using the local coffeehouse computers for internet access or the hotel lobby terminals for accessing the corporate LAN (e.g., for reading email), as keyloggers could have been installed on those devices).	Annually	COBIT PC5 Policy, Plans and Procedures

#	Rat-ing	Actions	Frequency	Documents to Consult

4.3	****	Check whether written and concise[2] policies are available to enforce corporate strategy. These policies should include:
		• Key and password management
		• Employment continuity
		• Employee termination
		• Substance abuse
		• Background checks
		• Trouble management
		• IS training policy
		• Employee hiring
		• Privacy policy
		• Security policy
		• Use of IT services for non-work related use
		• Telecommuting policy
		The policies should be published in the site's policy manual.
			Annually	BSI – S 2.192;
				Change in the Federal Data Protection Law 3.§ 4g.c) (2a);
				COBIT PC5 Policy, Plans and Procedures
				Guidelines regarding Internet and email surveillance at work;
				ISO/IEC 17799:2005 – Chapter 1, 2, 3, 5, 6, 7, 8, 10, 11.2 and 11.3;
				ISO/IEC 27001:2005 – Sections 4-8; S.B. 1386

4.4	***	Check whether records show that a disciplinary action is taken if an employee violates information security procedures or any of the policies outlined.	Quarterly	ISO/IEC 17799:2005 – Chap 13.1.1
4.5	***	Ascertain that there is an incident reporting procedure in place that encourages employees to report all insecure conditions and risky practices to their supervisors.	Annually and all new hires	BSI – S 2.193; ISO/IEC 17799:2005 – Chap 13

[2] Policies have to be as brief as possible to be meaningful and followed. Hence, a short 5-step guide for a fire alarm might be more effective than a 50-page document that nobody reads.

#	Rat-ing	Actions	Frequency	Documents to Consult
		Operational		
4.6	*****	Explain information security responsibilities to all employees and ensure that they understand them.	Quarterly and all new hires	NIST – SP 800-100 – Chapter 4; ISO/IEC 17799:2005 Chapter 8.2.2
4.7	****	Ascertain that managers, supervisors and workers are held accountable for information security, just as they are held accountable for quality.	Annually and all new hires	NIST – SP800-100 – Chapter 8.3 Rules of Behavior
4.8	****	Check whether appropriate records are kept of the training each employee has received.	Annually and all new hires	BSI – T2.49; ISO/IEC 17799:2005 Chapter 8.2.2

4.9	***	Train all workers to perform their jobs securely with regards to safeguarding data when using IT equipment (e.g., smartphone, BlackBerry, notebook, wireless connection at the neighbourhood coffee shop).	Annually and all new hires	COBIT – Deliver and Support – DS7 – Educate and Train Users;
				BSI – S 2.154, BSI – S 3.26;
				ISO/IEC 17799:2005 Chapter 8.2.2

5. Infrastructure Reliability and Dependability

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
5.1	****	Ascertain that procurement and deployment of new technology follows an acquisition profile for secure adoption of IPv6.	Annually	NIST – SP500-267 – Appendix D

5.2	***	Identify and initiate remedial actions based on information collated with the help of this Checklist and follow up with the:
		• Review and establishment of management response;
		• Assignment of responsibilities for remediation;
		• Tracking of changes and actions committed;
		• Control if changes did result in the improvements wanted as registered in subsequent audits;
		• Assess the effects upon performance metrics (see Section 7 below).
			Annually	COBIT – ME 1.6, ME2.7 Remedial Actions; 6.9 Network Management;
				NIST – SP500-267 – 6.9 Network Management;

5.3	***	Check whether system management plan is regularly reviewed and modified to meet engineering and programming changes and updates.	Annually	BSI – S2.169, S2.170, S2.221, S4.24

5.4	***	Check whether contingency planning and reliability of servers and networks follow best practices.	Quarterly	BSI – S6.69,
				NIST – SP 800-80 – Table 10. Contingency Planning (CP) Control-Specific Approach (p. 27);
				COBIT – DS 4 – Deliver and Support – Ensure Continuous Service;
				EBIOS – Section 5 – 3.4.14 CRH : Human resources – CRH_PDP.1.3;
				ISO/IEC 17799 Chapter 14.1.3

#	Rat-ing	Actions	Frequency	Documents to Consult
		Operational		
5.5	*****	Check whether logging of system resource usage is taking place, especially for critical operations (like accessing archive, data, changing records, or printing files).	Annually	BSI – S4.114; COBIT – DS5.5 Security Testing, Surveillance and Monitoring
5.6	*****	Investigate suspicious activity incidents and suspected violations that were reported in the audit findings.	Semi-Annually	COBIT – COBIT AI5.2, 4.9 DS8 Manage Service Desk and Incidents; Wagner & Gattiker, 2007, NIST – SP800-80 – Table 12. Incident Response (IR) Control-Specific Approach (p. 29)
5.7	****	Use and document best practice methods enabling checking that only authorized equipment can be connected to the network (e.g., filter for Mac address when providing access to wireless devices such as mobile phones, notebooks, preventing rogue wireless routers from being installed).	Semi-Annually	NIST – SP800-80 – Chapter 4
5.8	****	Control that physical access to servers meets best practice standards and none used server's ports are securely shut down (disabling their use by an unauthorized party).	Semi-Annually	NIST – SP800-80 – Chapter 4
5.9	****	Check whether web application security measures limit vulnerabilities in web application security.	Annually	BSI – S4.185
5.10	***	Control that archival procedures, security policy and data integrity are checked, tested and audited.	Semi-Annually	BSI – S 2.260, S4.81, S4.93 COBIT – DS4.9 Offsite Backup Storage; Sarbanes-Oxley Sec. 404. Management assessment of internal controls;
5.11	***	Confirm scalability of the system while assuring operational reliability.	Annually	COBIT – PO3 – Plan and Organise – Determine Technological Direction BSI – 7.10;

#	Rat-ing	Actions	Frequency	Documents to Consult
5.12	***	Confirm infrastructural reliability of the remote or mobile workstations.	Annually	BSI – S4.63; EBIOS – Section 5 – 3.4.14 CRH : Human resources – CRH_PDP.1.3

6. Platform and Services

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
6.1	***	Check if the safeguards protect confidentiality and accuracy of data at mobile devices (e.g., USB-sticks, mobile phones – all data are encrypted) and whether private equipment is adequate for meeting the same standards as corporate equipment	Quarterly	BSI – S4.114, S4.200; ISO/IEC 17799:2005 Chapter 10.4.1
6.2	***	Check the frequency by which system configuration requirements are implemented; whether published configurations are used; or otherwise justification has been provided why the enterprise is not doing so	Quarterly	BSI – S 2.25$
6.3	***	Check whether the firm's security measures include identifying the most threatened systems and ensuring that adequate defenses (such as hardware-based firewalls, server- *and* PC-based anti-virus, spam filter, content filter and anti-spyware software) are installed	Annually	BSI – S2.154, S2.155, S2.156, S2.159; COBIT DS5.9 Malicious Software Prevention, Detection and Correction
6.4	***	Ensure that operating systems, devices and applications are compliant with the Minimum Baseline Security Standards (MBSS) provided by industry and/or vendors, and that corresponding changes have been documented in the latest baseline configuration	Semi-Annually	NIST – SP800-80 – Chapter 5
		Operational		
6.5	*****	Check whether OS version, maintenance and patches (hotfixes) within the target are up-to-date.	Monthly	BSI – T2, S2.273 COBIT COBIT AI3.3 Infrastructure Maintenance

#	Rat-ing	Actions	Frequency	Documents to Consult
6.6	****	Check that critical software updates (e.g., Microsoft Office, Oracle, SAP) are part of a patch management that is centrally controlled and installed within the first week of release[3] .	Quarterly	COBIT AI3.3 Infrastructure Maintenance, DS5.9 Malicious Software Prevention, Detection and Correction
6.7	****	Check that a Group Policy Object has been written, installed and is being adhered to for mission-critical applications, such as the Windows Server Update Services[4], or databases, such as Oracle or SAP.	Quarterly	COBIT policy
6.8	****	Check whether all corporate-owned devices have been accounted for.	Monthly	COBIT DS11.3 Media Library Management System, DS13.4 Sensitive Documents and Output Devices
6.9	****	Check whether users do not have sysadmin privileges on their machines (i.e., cannot remove or install programs), as reflected by the role-based access management.	Monthly	COBIT – DS5 – Deliver & Support- DS5.4 User Account Management
6.10	****	Check whether datacenter inventory (including types of applications, systems run and software licenses used) have been regularly updated.	Quarterly	COBIT DS9.3 Configuration Integrity Review, AI7 Install and Accredit Solutions and Changes – AI6.5 Optimised

[3] In the ideal scenario, the patch should be installed on an isolated system and pre-tested before rolling it out over the network. If this is unfeasible, it is worth waiting a few working days before installing the critical patch. In fact, a vendor might be forced to either re-issue a patch or release an update after some customers could have been reporting as having severe problems with a critical patch.

[4] If there are multiple Windows Server Update Services (WSUS) servers, then there should be a Group Policy Object (GPO) for each WSUS server. If WSUS servers are shared by multiple sites, one can link each site to the relevant WSUS site's GPO.

As well, there is no need to create a GPO for every site, unless there is a preference for configuring other WUAU settings on a site-by-site basis.

If one has multiple sites, there is no need to create a separate GPO for each computer group, one can simply link to the relevant WUAU GPO that has already been created.

#	Rat-ing	Actions	Frequency	Documents to Consult
6.11	****	Based on the datacenter inventory, when security patches are being released, determine whether patches can be tested with the help of a centralized software management toolbox (e.g., Microsoft Systems Management Server) and quickly deployed, keeping patch latency to an acceptable minimum.	Quarterly	BSI – S4.44
6.12	***	Check whether the organization keeps a data inventory and securely deletes unneeded data.	Quarterly	BSI – Chap 1, S2.167
6.13	***	Check whether role-based access management and authentication solutions limit access to confidential information, and whether both private and public information are adequately protected.	Quarterly	COBIT – Acquire and Implement – AI2.4 Application Security and Availability; ISO/IEC 17799:2005 Chapter 10.4.1
6.14	***	Check whether work-related IM, VoIP, email traffics from work and remote locations (e.g., teleworkers) are archived and backed-up according to the regulations.	Annually	BSI – S4.114, S4.114, S4.168, S4.169, S4.170, S4.171, S6.47, S6.49, S6.50, S6.090
6.15	***	Check whether data are hosted on a system that meets applicable environment, connectivity and platform requirements.	Annually	COBIT – DS12 Deliver and Support – Manage the Physical Environment;
6.16	***	Check whether all PCs and notebooks have installed software-based firewalls, anti-virus and spam filtering obtained from a vendor different than the one providing server solutions.	Quarterly	BSI – S 4.151, S2.156, S2.159
6.17	***	Check whether solutions have been implemented to monitor and limit misuse of user IDs for Instant Messaging and the misappropriation of corporate domain names (i.e., by the imposters using IM).	Quarterly	ISO/IEC 17799:2005 – Chapter 10.10
6.18	***	Check that a Group Policy Object (GPO) has been written and is adhered to regarding updating critical software.		NIST – SP800-100 – Chapter 2.2.5 Information Security Policy and Guidance

7. Connectivity

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
7.1	****	Ascertain that new technology meets minimal mandatory IPv6 capabilities.	Semi-Annually	NIST – SP500-267 – Appendix D
7.2	***	Check whether electronic documents contain all relevant data, discoverable at acceptable cost and within a reasonable time frame, especially if asked to produce these in the court of law.	Annually	Amendments to the Federal Rules of Civil Procedures – Rule 16, Rule 26 (e-discovery); BSI – S4.114, S4.173, S5.25 Guidelines for the discovery of electronic documents in Ontario B – (ii) Preservation of Electronically Stored Documents, (iv) Production of Documents in Electronic Form;

7.3	***	Ensure that formal agreements are in place that specify the technical and security requirements for interconnecting information systems; define the responsibilities of participating organizations (e.g., Internet Service Provider, Outsourcer); and specify the rules governing these interconnections.	Annually	ISO/IEC 17799:2005 – Chapter 12.5.1 Change control procedures;
				ISO/IEC 27001:2005 – Annex A;
				EBIOS – Section 3 – CAL-03: Procedures for secure use of the organisation's telecommunication networks;
				NIST – SP 800-100 – Chapter 6

7.4	***	Develop a roadmap that will be followed for assuring that your information security management system meets methodological and security control requirements for certification.	Annually	ISO/IEC 27001:2005 – Sections 4-8;
7.5	***	If you wish to claim that your information security management system complies with a standard and get it certified by an accredited registrar, ensure that methodological and control measures are met according to the clauses of the standard.	Annually	ISO/IEC 27001:2005 – Sections 4-8
		Operational		

#	Rat-ing	Actions	Frequency	Documents to Consult
7.6	***	Check whether the company has recorded accurate and up-to-date network topology and configuration.	Quarterly	COBIT – DS5.10 Network Security; EBIOS – Section 3 – Technical Constraints, p. 16
7.7	***	Ascertain that OpenDocument Format (ODF) is being used to enable users of varying office suites to freely exchange documents and be compliant with the government agencies' requirement for supplying documents using ODF (e.g., revenue services).	Annually	ISO/IEC 26300 – ODF – OpenDocument Format OASIS standard

8. Process Management and Reengineering

#	Rat-ing	Actions	Frequency	Documents to Consult
		Strategic		
8.1	***	Compare and document how different vendor solutions (e.g., Enterprise Resource Planning – ERP) facilitate improving accuracy, consistency and transparency of decision-making processes.	Inititial tendering and system evaluation process	AAADM Better Practice Guide, Part 2-3
8.2	***	Establish baseline security, accuracy and accountability metrics for the information system or software (see also Section 2 regarding metrics).	Before initial implementation	AAADM Better Practice Guide – Part 4-6 NIST – SP800-100 – Table 9. Configuration Management (CM) Control-Specific Approach
8.3	*****	Ascertain that baseline security, accuracy and accountability metrics reach the benchmarks as specified in the purchase agreement or tendering documents submitted by vendor.	During initial implementation and annually thereafter	AAADM Better Practice Guide – Part 6; NIST – SP800-100 – Chapter 7
		Operational		
8.4	****	Ensure the continued accuracy and accountability of information systems, especially considering possible changes to the underlying legislation, policy or procedures.	Annually	AAADM Better Practice Guide, Appendix B: ARC Best-Practice Principles; NIST – SP800-100 – Table 7. Audit and Accountability (AU) Control-Specific Approach

Disclaimers

Material in this Checklist does not have any legislative authority and is published only for user convenience. It should not be construed as legal advice for any particular applications or circumstances. The authors are not responsible for its use in the field.

The materials in this document have been compiled from internal and external sources and are provided solely for reference purposes. This Checklist might change due to regulatory developments as well as evolving best practices. It is intended to serve as a starting point only, and should be tailored to meet enterprise's specific requirements.

While the authors have attempted to provide accurate information, no representation is made or warranty given as to the completeness or accuracy of the materials. In particular, you should be aware that the materials might be incomplete, contain errors, or have become out of date. You should therefore verify information obtained from this document before you take any action upon it.

Urs+Nahum's Security Checklist: Staying Current with the Latest Developments and Updates

In this document we are trying to help you to stay current with the latest threats and security solutions, pertinent regulations, standards, and critical guidelines that are frequently changed by the regulatory agencies.

Our team can also help you by providing complementary and customized subscriptions to the latest information on critical security-related regulations and policies, such as:

- Zero-day exploits that are being spread across the Internet and actively exploited by malicious users (*http://casescontact.org/zeroday_list.php*)
- Alerts and advisories about the latest threats, patches and work-arounds (*http://casescontact.org*)
- Information about IT security tools and trends, malware, NIST privacy and security metrics, and spyware (*http://blog.cytrap.eu*)
- IT security and risk management – regulatory changes, legal compliance, audit regulation, standards, financial controls, best practices (*http://regustand.CyTRAP.eu*)

You can subscribe to the above information via email or RSS. The news comes either in the stream of individual messages (RSS or email) or condensed in a weekly digest / newsletter (email). If you wish to subscribe to several online newsletters just visit:

http://CASEScontact.org/subscribe_all.php

Let Our World-Class Team Work with You

Our team could help your organization to protect your network with the services that include development of security and network maintenance policies, metrics and benchmarking, conducting audits, as well as compliance reporting and incident handling. We are unique in helping executives to link up corporate business goals with comprehensive security and network maintenance measures and practices.

We also specialize in the development of leading-edge Vista 64-bit based low-cost, high-security and offsite-managed services for corporate networks, typically deployed in the regulated financial industry.

Baseline Review

A review (which at the initial stage is not an audit or an inspection) typically starts with an assessment of the maturity of the organization's IT security program. It includes evaluation of the enterprise's IT security policies, procedures, security controls, implementation and integration across all business areas.

Our team performs a review of the agency's organizational structure, culture, and business mission. After the assessment is performed, the team documents critical issues identified during the assessment phase and provides corrective actions associated with each issue.

The corrective actions are then provided as a prioritized action plan for the agency to improve its computer security program. The resulting action plan is weighted to provide the organization with the substantive improvements in the most cost-effective way.

The action plan can readily be used to develop scopes of work for quick bootstrapping of the cyber security program.

Audit and Compliance Review

Our security audit focuses on testing and ensuring that your enterprise's assets are fully protected according to regulatory and compliance requirements. As well, we test whether your defenses are able to meet best practices and standards with cost-effective processes and methods.

Our team's audit and compliance report covers every aspect of the client's policy, pointing out gaps in the organization's defenses and perimeter security.

Corrective actions are then provided as a prioritized action plan for the client that improves security and assures compliance.

Corrective Actions and Improvements

To promote accountability, integrity, and efficiency, an organization might require improvements for its security position and compliance.

We can help you improve your compliance reporting. By leveraging our advanced technology, processes, and methodologies, our team can empower your organization to better manage your security and compliance efforts.

Regular Check-up Services

Our team can also provide virtual services for your organization on an ongoing basis, such as the role of privacy officer, compliance officer and security officer.

For such virtual services we conduct regular monitoring, as well as an annual compliance review and/or audit, to ensure that your corporate policies and procedures are adequate and up to date with current standards and regulations. The annual compliance review is submitted to management and the board to ensure that appropriate measures have been taken to ensure regulatory compliance.

Contact Us

Our team is international, with presence in Europe and North America, and is made up of highly qualified and experienced professionals that provide the best quality services to our partners and clients. Services are available in English, French, German, Danish, Hebrew, Russian and Ukrainian.

Contact:

Urs E. Gattiker, PhD (see contacts and bio at *http://info.cytrap.eu/?page_id=2*):
Email: *Urs+Nahum-Checklist at CYTRAP.eu*
Phone: +41 (0)44 272-1876 or +41 (0)76 200 77 78

Acknowledgements

The authors are thankful to Freydun Michael Badri, Tom Buschman, George Carter, George Dask, Mich Kabay, Yuri Melamed, Prateek Srivastava, Monte Robertson and Andreas Wagner for their valuable contributions to this document.

Updates

Make sure the version you use is the latest one, check with the link below for a FREE download.

CyTRAP ID	ISBN 978-0-9783768-0-2
Version Date	2007-05-30
Verify that you have latest version	*http://ReguStand.CyTRAP.eu/?p=1*

References

These have been structured in several sub-sections. Space limitations made it impossible to list every law, regulation, standard, best practice or checklist. Instead we have selected authoritative, comprehensive and detailed documents that Checklist users could effectively employ when structuring their ongoing security defenses.

Legislation

(State-Enforced Mandatory Requirements)

Amendments to the Federal Rules of Civil Procedures – Rule 16, Rule 26 (e-discovery) [*http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf*] Last access: 2007, March 10]	On April 12, 2006 the United States Supreme Court approved the proposed amendments to the Federal Rules of Civil Procedure that address the discovery of electronically stored information (ESI). Understanding what ESI one has stored, where and how is vital to successful negotiation of a discovery plan. In turn, successful negotiation of that plan is vital to effective litigation management, strategy and enforcement.
Neuordnung des schweizerischen Revisionsrechts (OR) – Art. 727 ORE: (Art 728a Abs. 1 Ziff. 3 OR) (Realignment of the Swiss Code of Obligation – CO – Art 727 CO: (Art 728a Para 1 Nr. 3). Bern, CH: Swiss Federal Government. [*http://cytrap.org/RiskIT/mod/glossary/view.php?id=12&mode=entry&hook=606* Last access: 2007, April 25]	This Swiss regulation is supposed to go into force in late 2007. It postulates that the board of directors is responsible for a regular and systematic risk assessment. Internal control procedures must be formalized, documented and reviewed annually by external auditors. The regulation requires the company's auditors to attest to, and report on management's assessment of the effectiveness of the internal controls and procedures for financial reporting (including risks, IT security and privacy) in accordance with the standards established.
SB 1386: California Security Breach Information Act (SB-1386) [*http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=0102&house=B&site=sen* Last access: 2007, March 10]	This law is probably the first legislation that addresses data security breach issues. A breach might occur when a laptop containing customer or employee data is stolen or lost. The Act outlines under which conditions such a breach might have occurred and within what time frame after discovering the affected parties (e.g., customers, students, suppliers) must be informed.

Sarbanes-Oxley Act 2002. (2002) [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf Last access: 2007, March 10] For more information see: *http://www.sec.gov/news/press/2003-66.htm*	Sarbanes-Oxley Act is a seminal US federal legislation that established new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Section 404 of the Act directs the enterprise to ensure that the annual report contains (1) a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) management's assessment of the effectiveness of the company's internal control structure and procedures for financial reporting. Section 404 also requires the company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with the established standards. Some experts estimate that Section 404-related tasks consist of about 70% of IT security and system-related matters.

The Combined Code on Corporate Governance[5] (June 2006). London, UK: Financial Services Authority (FSA). [*http://www.fsa.gov.uk/pubs/ukla/lr_comcode2003.pdf* Last access: 2007, March 10]	The Listing Rules require listed financial companies in the UK to make a disclosure statement in two parts in relation to the Code. In the first part of the statement, the company has to report on how it applies the principles in the Code. In the second part of the statement the company has either to confirm that it complies with the Codes provisions or where it does not to provide an explanation. The Combined Code provides the framework and structure for corporate governance that helps improve internal controls.

[5] The key governance principles – the specific responsibilities for the governing board of an organization – are as follows: setting strategic aims, providing strategic leadership, overseeing and monitoring the performance of executive management, and reporting to shareholders on their stewardship of the organization.

The UK's Combined Code on Corporate Governance revised in 2003, Switzerland's Realignment of the Swiss CO – Art 727 CO: (Art 728a Para 1 Nr. 3 CO) (2006), the OECD's Principles of Corporate Governance (1999), the Bank of International Settlements' Enhancing Corporate Governance in Banking Organizations (also 1999) and the USA's Sarbanes Oxley Act of 2002, together with OECD, Canada, Germany and other countries' privacy regulations, provide the framework and structure for accountability activities that are driving corporate boards and regulators toward a common understanding of effective governance.

Privacy and information security-related efforts are likely to take by far the majority of the action required to assure legal compliance and achieve effective governance.

Erstes Gesetz zum Abbau buerokratischer Hemnisse insbesondere in der mittelstaendischen Wirtschaft. Artikel 1. **Aenderung des Bundesdatenschutzgesetzes** (Change in the Federal Data Protection Act – Germany) (August 22, 2006). **Bundesgesetzblatt Teil 1**; Nr. 40. *http://217.160.60.235/BGBL/bgbl1f/bgbl106s1970.pdf* Last access: 2007, March 10]	British-based watchdog group Privacy International ranked 36 countries in early 2007. Germany and Canada were the only two countries to be given the status of having significant privacy protections and safeguards. Germany's Federal Data Protection Act (FDPA) is very specific about when a privacy officer with appropriate qualifications is required (e.g., if nine or more employees have access to personal data – privacy officer position must be established). Frequently, SMEs appoint an external expert to act as privacy officer. The privacy offier's annual report must address legal compliance and be published (e.g., online and in printed form). Audit findings (i.e. privacy officer's written report) must be made available to shareholders, customers, as well as the public[6]. Privacy protection is seen as an instrument for achieving competitive advantage in the global marketplace.

[6] The FDPA stipulates that priority will be given to products in tenders by public bodies, whose compliance with the privacy protection law und data security is set out in a **formal procedure**.

Standards
(Providing a Framework)

ISO/IEC 15408-1:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model [*http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip* Last access: 2007, March 25].	This standard is used as a reference for security evaluation and certification of IT products and systems. It defines IT security functional and assurance requirements. The Common Criteria ISO/IEC 1528 standard provides the underlining method that includes uniform comparisons, response to changes in current application and security conformance to best practice. Whereas ISO/IEC 17799 is a code of practice for information security management, ISO/IEC 15408 focuses on security requirements.
ISO/IEC 17799:2005 (2007 to be renamed ISO/IEC 27002) Information technology – Security techniques – Code of practice for information security management (based on BS 7799-1/ISO/IEC 17799:2000) (2005). [*http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=* Last access: 2007, March 10] More info: *http://en.wikipedia.org/wiki/ISO/IEC_17799*	One of the most influential information security standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), based on the British Standard (BS) 7799-1:1999 and having direct equivalents in the number of developed economies. ISO/IEC 17799 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).
ISO/IEC 27001:2005 – Information technology -- Security techniques -- Information security management systems – Requirements [*http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3=* Last access: 2007, April 5]	ISO/IEC 27001 is an information security management standard that helps organizations to establish and maintain an Information Security Management Systems (ISMS). Hence, it applies to all types of organizations, regardless of their business or size. ISO/IEC 27001 defines the implementation requirements based on ISO 17799 and can be used by companies to build a security plan. More important, it contains verifiable implementation language that spells out procedures and practices that an auditor can use to determine whether the organization is compliant.

ISO/IEC 26300 – ODF – OpenDocument Format OASIS (Organization for the Advancement of Structured Information Standards) [*http://opendocument.xml.org/* Last access: 2007, March 10]	OASIS is an international e-business standards consortium that has developed the Open Document Format for Office Applications. It introduced a new XML-based file format that describes electronic documents, such as e-books, spreadsheets, figures, presentations or text files. ISO/IEC 26300 enables file sharing regardless of the operating system platform or software used. Most European Union Member States have stipulated that this standard must be used for all documents issued and or received by the public agencies by or after 2008. For instance, in March 2007 the French Defence Department made public that: "Open standards and open formats will be adopted for new IT systems, and for important changes in the existing systems."

Specifications and Procedures

(Providing Detailed Guidance on Mandated Actions to Comply with Legislation)

Bowen, P., Hash J., & Wilson, M. (October 2006). **Information Security Handbook: A Guide for Managers** (SP800-100). Washington DC: National Institute of Standards and Technology (NIST). [*http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf* Last access: 2007, March 10]	This authoritative guide helps managers to address the requirements of various US security policies and laws, such as the Clinger-Cohen Act of 1996 and the Federal Information Security Management Act (FISMA). The guidelines are sufficiently generic, allowing organizations to tailor security defenses to their specific technical and business requirements.
Chew, E., Clay, A, Hash, J, Bartol, N. & Brown, A. (May 2006). **Guide for Developing Performance Metrics for Information Security** (Draft SP800-80 DRAFT). Washington DC: National Institute of Standards and Technology (NIST). [*http://csrc.nist.gov/publications/drafts.html#sp800-80* Last access: 2007, March 10]	This guide is intended to assist organizations in developing metrics for an information security program. The methodology links information security program performance to the agency or organizational performance. It leverages agency-level strategic planning processes and uses security controls from NIST SP 800-53. To facilitate the development and implementation of information security performance metrics, the guide provides templates, including at least one candidate metric for each of the security control families described in NIST SP 800-53.
Nightingale, S., Montgomery, D., Frankel, S., Carson, M. (2007). **A profile for IPv6 in the U.S. government – Version 1.0** (Draft SP500-267). Washington DC: National Institute of Standards and Technology (NIST). [*http://www.antd.nist.gov/usgv6-v1-draft.pdf* Last access: 2007, March 15]	NIST requires conformance testing for IPv6-based IT infrastructure, such as routers, and security network devices. The guidelines are sufficiently generic, allowing organizations to tailor security defenses to their specific technical and business requirements.

Codes of Practice

(Providing a Detailed Framework for the Procedures that should be Followed)

BSI (April 2004). **BSI IT Grundschutz Manual** [BSI IT baseline protection manual) Bonn: Bundesamt fuer Sicherheit in der Informationstechnik (Federal Office for Information Security (BSI) – Germany)] [*http://www.bsi.bund.de/english/gshb/manual/index.htm* (English Version) Last access: 2007, March 10]	Produced by the German Federal Government, this manual presents a set of standard security measures that apply to virtually every IT system. It provides standard security measures for typical IT systems with "normal" protection requirements, description of safeguards, processes that must be implemented to achieve satisfactory security levels and obtaining baseline data for security metrics. The manual offers an exhaustive and very detailed framework for achieving medium-level protection against generic threats.
Control Objectives for Information and Related Technologies (COBIT) **4.1**. (2007) Rolling Meadows, IL: IT Governance Institute [*http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981* Last access: 2007, March 10]	COBIT is an internationally recognized framework for the preparation of specific audit plans and programs. It standardizes the review and internal control criteria for IT processes and information. Executive guidance about the corrective measures that should be adopted can be developed based on the findings. The manual offers an exhaustive and detailed framework for auditing generic information systems in relation to the security baseline.
EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité (Expressing Needs and Identifying Security Objectives) (January 2004). Paris: Secretariat General de la Defense National. [*http://brief.weburb.dk/frame.php?loc=archive/00000244/* (in English) Last access: 2007, March 10] More info: *http://blog.cytrap.eu/?p=194*	EBIOS' main objective is to allow organizations, including public agencies, to determine the security actions that should be undertaken to better manage risks, security and confidentiality of information assets and data. EBIOS was published in 1995 by DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), a French government agency that continues to maintain and improve the EBIOS methodology. It also includes software that can be used to take advantage from the EBIOS methodology.

Guidelines and Best Practices

(Providing Guidance on How to Comply with the Legislation)

Automated Assistance in Administrative Decision-Making Working Group (2007). Automated assistance in administrative decision-making better practice guide. Canberra: Commonwealth of Australia, Department of Finance and Administration Australian Government Information Management Office, Office of the Commonwealth Ombudsman, Australian National Audit Office, Office of the Privacy Commissioner. [*http://www.agimo.gov.au/publications/2007/february/aaadm* Last access: 2007, May 1]. Complete guide: [*http://www.agimo.gov.au/__data/assets/pdf_file/56107/AAAADM_Better_Practice_Guide.pdf* Last access: 2007, May 1]. Pocket guide: [*http://www.agimo.gov.au/__data/assets/pdf_file/55583/AAADM_Pocket_Guide.pdf* Last access: 2007, May 1].	The AAADM Better Practice Guide emphasizes that IT systems applying new technologies making administrative decisions must be supported by appropriate business practices. More important, the practical advice as well as the checklists provided should help in ensuring that new systems used to produce decisions affecting individuals, customers, suppliers and shareholders are fair, accurate, and open to audit and review. This guide is useful for analyzing processes and operational steps to be mechanized. Thereafter, one can assess how the newly purchased and installed system or software helps improving business practices, accountability and makes them more open to audit and review as a part of good corporate governance (e.g., Enterprise Resource Planning – ERP).
Gattiker, U.E. (2006) **CyTRAP.org/RiskIT – The 3 greatest risks with outsourcing knowledge processes**. Zurich: CyTRAP Labs. [*http://cytrap.org/RiskIT/file.php/3/2006/CT31RIT0002-Outsourcing-KnowledgeProcesses.pdf* Last access: 2007, March 20].	The article outlines risk management effort that is required for outsourcing and explains why Service Level Agreements (SLA) cannot and would not protect the client against many risks, especially when using offshoring. The document provides a framework that allows organizations to tailor security defenses to their specific technical and business requirements.
Gattiker, U.E. (2007). **CyTRAP Labs – Developing a holistic security strategy.** Zurich: CyTRAP Labs. [*http://blog.cytrap.eu/?p=206* – Last access: 2007, May 28].	The article explains that while the strategy for managing risk and security might be critical, sometimes small practical steps (e.g., policies regarding privacy, encryption, mobile computing and disposing of data/hard disks) are the foundation needed before a holistic security policy can be defined and implemented. The document provides a framework that allows organizations to tailor security defenses to their specific technical and business requirements.

Goldmann, N. and Orton, E. (2002). The critical role of independent security audits. In P. B. Lowry, J. O. Cherrington and R. R. Watson (eds.), **The E-Business Handbook** *(Chapter 20, pp. 353-363)*. Bacon Raton, Fl: CRC Press [*http://www.addsecure.net/inform.asp#Publications* Last access: 2007, April 20].	To uncover the weak links, the security of every participant in an ecommerce service must be periodically audited. As organization's financial audits are always conducted by an independent source, so too should its security audits. Only independent and impartial tests can validate corporate security efforts, ensure that all potential security problems have been examined and exposed, and provide the service's clients with objective proof that sufficient due diligence has been exercised in securing their data. An independent audit can also help an organization to protect the integrity of its network and, in the process, avoid worthless security expenses by focusing security resources on the vulnerabilities discovered. The results of an independent audit also add credibility to the service provider's claims that its Web site is secure.
Guidelines for the discovery of electronic documents in Ontario. Toronto: Ontario Bar Association. [*http://www.oba.org/en/pdf_newsletter/E-DiscoveryGuidelines.pdf* Last access: 2007, March 10]	The guidelines provide litigation guidance on the extent of parties' obligation to produce electronic documents and information. Courts might apply these or locally prevalent guidelines in deciding what information parties must produce and how this production must be accomplished. The document provides a detailed framework that allows organizations to tailor security defenses to their specific technical and business requirements.
Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz. Für öffentliche Verwaltungen und Privatwirtschaft (Guidelines regarding Internet and email surveillance at work. For public and private sector enterprises) – Version 2.0 (Dec. 2003). Berne, Switzerland: Der eidgenössische Datenschutzbeauftragte (The Federal Privacy Commissioner) [*http://www.ch.ch/private/00085/00091/00499/00500/index.html?lang=de&download=M3wBPgDB/8ull6Du36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN2gX+DbKbXrZ6lhuDZz8mMps2gpKfo* Last access: 2007, April 7]	Swiss federal guidelines that outline under which conditions Internet mail can be checked and when and why the use of Closed Circuit Television (CCTV) for surveillance and crime control might not be allowed. CCTV is used extensively in the UK but generally not allowed in Germany (e.g., for 2007 German Constitutional Court ruling against the use of CCTV cameras in the public spaces see *http://blog.cytrap.eu/?p=209*). The document provides a very detailed framework that allows organizations to tailor security defenses to their specific technical, regulatory and business requirements.

Wagner, A. & Gattiker, U. E. (2007). **Ueber den Sinn und Unsinn von Penetrations-Tests** (About Sense and Nonsense Regarding Penetration Testing). Zurich: CyTRAP Labs. [*http://info.cytrap.eu/?page_id=26* Last access: 2007, May 20]. [*http://info.cytrap.eu/?page_id=25* Last access: 2007, May 24 – English Version].	The document outlines why classical intrusion detection and penetration testing fails to provide the information needed for a comprehensive risk assessment as suggested by EBIOS – cited in this document. The document provides a framework that allows organizations to tailor security defenses to their specific technical and business requirements.
Your privacy responsibilities. A guide for businesses and organizations. Canada's Personal Information Protection and Electronic Documents Act (PIPIDA) (March 2004). Ottawa: Office of Canada's Privacy Commissioner [*http://www.privcom.gc.ca/information/guide_e.asp* Last access: 2007, March 10]	The guide includes examples of how data protection and privacy legislation can be administered in a corporate setting. It suggests necessary approaches, checks and balances to be compliant, while keeping things simple. The document also provides a detailed checklist that allows organizations to tailor security defenses to their specific technical and business requirements.