

# Information security compliance

by IsecT Ltd. 3<sup>rd</sup> March 2011

## Executive summary

Wherever we operate we must comply with certain legal, regulatory and contractual obligations relating to information security in order to avoid prosecution/regulatory action, fines and adverse publicity. The obligations are complex and change frequently. We must continue to monitor and respond to the legislative and regulatory situation, and adopt security standards where commercially advantageous.

## Introduction

As has been famously said, the nice thing about standards is that there are so many of them from which to choose. You probably have a dim awareness of a whole alphabet soup of acronyms having something to do with security. Which security framework is most appropriate for you? What can frameworks help you achieve? And where do Treadway and Turnbull come into it?

The term "security framework" has been used in a variety of ways in the security literature over the years but recently it came to be used as an aggregate term for the various documents and associated programs from a variety of sources, that give advice on topics related to information security, in particular with regard to the planning, managing or auditing of overall information security practices for a given organization. In addition, there are several laws, regulations and standards imposed by governments and other authorities which may or may not impact on how you run your IT.

Some of these texts are guidelines specifically addressed towards information security, such as the ISO/IEC 27000 ("ISO27k") family of standards. In this category are also items such as the (free, both of charge and of access) publications and materials prepared by the United States National Institute of Standards and Technology (NIST). There have been a number of projects that attempted to produce similar sets of standards or practice lists, such as the now moribund CASPR (Commonly Accepted Security Practices and Recommendations), two versions of GASSP (Generally Accepted System Security Principles): these listed undertakings have been amalgamated into GAISP (Generally Accepted Information Security Principles).

Other frameworks are only peripherally related but have come to be seen as having a bearing on IT, systems or information security. Probably the most widely known are the auditing standards and outlines such as COBIT, and the variety of supporting documents and processes that have grown up around the United States' Federal Information Systems Management Act (FISMA). Others are more distantly associated, such as the Common Criteria for Information Technology Security Evaluation. Still others are even more tenuously connected, such as the advice on fraudulent financial reporting from COSO. (The various financial frameworks, laws, instructions and standards are generally concerned with the accuracy and reliability of reported earnings and the financial health of a company: ever since the demise of the quill and ledger, this naturally has significant implications for the management and control of data and information systems.)

Some frameworks are more specific, both in intent and application. The payment card industry has established its own data security standards. If you process credit card payments, you must conform to PCI-DSS. The United States' law known as SOX effectively imposes security requirements upon financial information systems.

These and other laws, regulations and standards have given greater urgency to the issue of compliance, moving towards the top of senior management's agenda. While you may view the incessant focus on compliance as an enormous pain in the butt, it can actually be to your

advantage to learn about the various security frameworks and help make sure that they are applied rationally and sensibly, being cognizant of their respective strengths and weaknesses.

## General types and differences

Security frameworks come from a variety of sources and address a number of objectives. How relevant a specific framework will be to your organization, its operations and situation, will depend partly upon your enterprise and partly upon the aims and objectives of that framework. This is not to say that a specific framework may not have relevance to your enterprise. Nevertheless, there are certain characteristics that tend to be consistent across many of the frameworks.

All frameworks give management different pieces of information about your systems, processes or operations, and all such information may be valuable. In some cases, the initial intent of the framework may be irrelevant. For example, most of the financial frameworks and instructions address the issue of fraudulent reporting of the financial wellbeing of the company. To this end, they generally concentrate on requiring the disclosure of the availability and status of internal financial controls against fraud *etc.* within the company. Internal controls are part-and-parcel of information system security, so these frameworks can provide useful guidance even though their original purpose is strictly outside the realm of infosec\*.

## Governance frameworks

There is widespread confusion in regard to the term 'governance' and what differentiates it from management. Some note that management might be said to increase direct performance, while governance may, through analysis, redirect activities to greater effect. (In a sense this only moves the question back one level: this simply seems to be the distinction between strategic and operational management.) In fact, if a distinction is being made, governance relates to the more static aspects, such as defining appropriate organizational structures and reporting lines, whereas the separate field of management is more related to controlling and directing operations.

Some texts note that five basic classes of decisions must be made in IT (principles, architecture, infrastructure, business application needs and the prioritizing of investment) and that these constitute the areas of governance. Again, this outline helps but does not get us much closer to a useful or functional definition. Architecture, to take a closer look at one aspect, is stated to be a level of abstraction above design but this definition also is not very helpful. A more functional description may be that architecture involves integration and standardization, but even this doesn't give us an awful lot of help in deciding what an information technology architecture is, nor what the governance of it may be.

Security frameworks that stress "governance" tend to a strategic management/overview perspective. Frequently they provide only a very generic structure for examining even the macro levels of a large enterprise, leaving mere details to be dealt with elsewhere. Such tools may be valuable for ensuring that information security is assessed in an holistic manner as part of corporate management and that large areas are not missed in the pursuit of small details, but they will not be of much practical use to those who need to start on securing particular systems. Today.

## Security frameworks

A number of security frameworks are primarily sets of divisions of security-related activities and functions. These are, in fact, the most likely to use the word "framework" in their titles and

---

\* It is rather ironic to note that if officers are willing to lie about corporate finances, they would probably have no compunction in regard to lying about the state of internal controls, or indeed their own expenses claims. Therefore, financial frameworks and compliance therewith may have even greater relevance to information security and audit than was their original aim.

descriptions. They define structures that provide for the breaking down of the overall organization and operations of an institution into smaller areas that may aid in the analysis of specific risks, security requirements and weaknesses. Thus, instead of balking at the thought of trying to analyze security requirements for your entire enterprise, the breakdown provides smaller and more manageable chunks for you, your colleagues and managers to digest.

### *Security standards*

Aside from internal security standards that an organization might prepare and adopt privately, there are many public security standards, ranging from relatively general security guidelines (such as the ISO/IEC 27000 standards) to highly specific and often deeply technical specifications (such as AES, the Advanced Encryption Standard). Since standards are mostly discretionary rather than mandatory in theory, they may not impose quite the same obligations as the laws and industry regulations noted below, but in practice there may be little option but to comply. Commercial pressures can be highly effective: WiFi equipment manufacturers who chose not to support the WPA2 security standard, for example, would probably not sell as many boxes as their competitors who do.

Some of the bodies responsible for information security standards are as follows:

- **ANSI** (American National Standards Institute) produces the “X9” family of security standards;
- **EESSI** (European Electronic Signature Standardisation Initiative). The European ICT Standards Board, part of the European Commission, launched this industry initiative bringing together industry and public authorities, experts and others in support of the European Directive on electronic signatures;
- **IETF** (Internet Engineering Task Force) produces Internet inter-operability standards, some of which cover security issues such as authentication and encryption;
- **ISACA, ISF and ISO/IEC** are mentioned elsewhere in this briefing;
- **ITU-T** is part of the ITU (International Telecommunications Union), itself part of the United Nations. It originated the X-series standards which are a significant element of the OSI (Open Systems Interconnect) standards;
- **NERC** (North American Electric Reliability Corporation) provides ‘reliability standards’ for the US electricity industry. Information security is a growing concern for the Supervisory Control and Data Acquisition (SCADA) systems and networks monitoring and controlling large parts of critical infrastructure, especially given the potential threat of terrorist or nation state attacks. NERC and in fact the whole industry is facing pressure to adopt NIST’s more stringent and comprehensive security standards;
- **NIST** (National Institute of Standards and Technology) produces a wide range of IT guidelines for the US Government. The **Special Publications 800-series** standards are particularly noteworthy for being comprehensive, detailed and well-written information security standards. There are currently about 150 SP 800 standards.
- **OECD** (Organization for Economic and Cultural Development)’s **Guidelines for the Security of Information** lay out nine principles for the deployment of information systems and five strategies to apply the principles. Their **Guidelines for Cryptography Policy** define principles for the development of national policies on cryptography including private use of cryptography, support for cryptographic research and lawful access.

### *Security checklists*

A significant number of security frameworks are presented in checklist form. This preference for the checklist format is hardly surprising: security does not normally involve a single function but rather a collaboration between related functions, along with a framework to help them work effectively together. Indeed, it is frequently pointed out that tremendous expenditures on security

may be entirely obviated by the lack of a single control, therefore a checklist of concerns to be covered by each function makes a great deal of sense.

Checklists, however, vary in content, intent and depth. One checklist may be based on functional security, another may deal with audit and assurance mechanisms, while yet a third proceeds from an examination of business functions. The level of detail also fluctuates from framework to framework. Highly detailed and specific information security frameworks might as well be written in hieroglyphics as far as most managers are concerned.

When using checklist-type frameworks, it is probably best to use more than one and choose complementary documents that approach security from alternative perspectives. The use of multiple resources is probably more important with checklist frameworks than with other types since there would be a psychology expectation of being "finished" once one had completed such a list. Just as there is no "one size fits all" security, there is no "one checklist fits all" universal security framework.

### 'Menus' of security controls

Most security professionals probably view security checklists in terms of lists of required security controls but surprisingly few formal security frameworks actually specify controls. Look for yourself. Many simply list broad areas of concern, prompting users to consider each realm and somehow (often through some unspecified process) decide which controls are actually appropriate.

In planning and considering the types of controls that we have, their effectiveness and new ones we may need, it may be helpful to categorize controls. Controls may for example be administrative (such as policies and procedures), physical (mostly barriers) or technical/logical. Information security pros tend to fixate on the last area and neglect the others.

A classification developed from the normal divisions of responsibility in business would list controls as management, physical plant or operations. ISO27k (see below) talks of 'risk treatments' that involve reducing, avoiding, transferring or accepting information security risks. Other divisions are equally useful. Corrective controls are applied when others have failed, directive controls provide guidance, deterrent controls use social pressures to reduce threats from human attackers, detective controls determine that a breach has taken place, preventive controls reduce our vulnerability to threats, recovery controls assist us to resume operations after an incident, and compensating controls provide coverage where others have been insufficient (compensating controls may perhaps be summed up in the phrase *defense in depth*). This partition of security actions has its roots in military and law enforcement studies.

For any given IT system or process, a wide variety of controls can be used. Indeed, a conglomeration of safeguards may be needed for a single process, system or structure. The finer grading and codifying of controls that we can do, the better our analysis of our total security posture will be. One method\* involves using different (orthogonal) classifications as the basis to generate a controls matrix, which can be used to assess the completeness of protection for a given system.

At some point it may become difficult to see the forest for the trees: having established a number of countermeasures, the practitioner may wonder at the necessity of mitigating further, somewhat obscure or seeming unlikely risks.

There are, of course, a number of tools for establishing the completeness of a risk management strategy, primarily involved with identifying specific risks (generally meaning the coincidence of threats acting on vulnerabilities to cause impacts). The controls matrix offers a slightly different kind of assessment of overall protections, noting broad classes of coverage and potential blind spots. The controls matrix is, therefore, a kind of security framework (as noted earlier) directed at the controls themselves.

---

\* If you're keen, details of this approach may be found in volume 3 of the 5<sup>th</sup> edition of the "Information Security Management Handbook", pages 179-182.

## Risk management and risk assessment frameworks

There are numerous standards, products, procedures, outlines and systems dedicated to the assessment, analysis and management of risks. They tend to fall into three categories: those specific to information systems and security, those dealing with general business risk and those from the financial (particularly the investment management) community. Those dealing with information security and business risks tend to be similar in structure and general outline, with some minor variations in terms of specifics to be addressed. The banking world looks at risk management in a very different way: there is a great emphasis on the single issue of solvency and capital reserves, with everything else (pretty much what information systems and business people would know as the entire field of risk management) being relegated to a separate category of operational risk.

Risk management frameworks are very much process-oriented. Structures of committees, information gathering and documentation are major aspects of these entities. If you are aware of deficiencies in regard to management structures and reporting in your own security environment (which is itself a risk), a risk management framework will likely be of benefit.

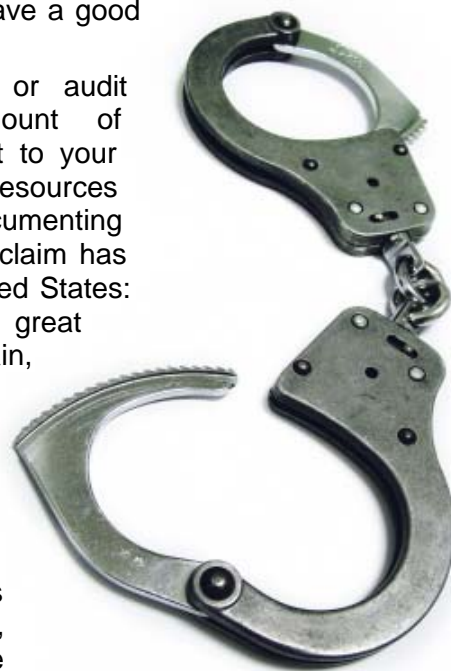
## Audit and assurance frameworks

A significant number of frameworks are concerned with audits since auditors generally need something definitive against which to audit. Audit and assurance frameworks stress points that can be measured and demonstrated or proven, but may have little to do with the actual security environment or situation. Most emphasize what can be proven objectively, discounting that which can only be surmised or subjectively assessed. It is always a good idea to pay attention to what can be measured and documented. It is very easy to say that we know we are secure but just haven't bothered to write it down. If you haven't documented it, or even worse can't document it, you really don't have a good idea of your situation.

At the same time, be careful of frameworks or audit approaches that require an excessive amount of documentation which may not be entirely relevant to your situation or needs. You may commit resources disproportionately to *proving* rather than *doing* - documenting for documentation's sake, creating red tape. This claim has been leveled at the Sarbanes-Oxley law in the United States: the expense of documenting internal controls in great detail competes with, and perhaps threatens to drain, the budget for security operations and other equally important aspects of information security management.

## Legal and regulatory frameworks

Given growing public awareness of the risks resulting from inadequate information security, legislators and official industry regulators are increasingly mandating a number of information security controls on organizations to supplement 'self-regulation'. It is important that organizations are aware of their compliance obligations, especially if they do business in multiple countries, deal with foreign customers, suppliers or partners, or handle confidential data belonging to third parties.



**IGNORE**  
**SECURITY LAWS & REGULATIONS**  
**AT YOUR PERIL!**

Worldwide there are literally hundreds, probably thousands of laws and regulations that in some way impact those gathering, processing, storing and communicating information. Thankfully, relatively few of them are directly and specifically concerned with information security controls: most are broader in scope, focusing on information content. However, they all need to be assessed and monitored and, where relevant, complied with.

Some security frameworks carry the force of law or regulatory mandate – those concerned with privacy, for example, often impose security obligations on organizations. Non-compliance can result in fines for organizations, sometimes even jail terms for their Officers. Some industry regulations are advisory in nature but in practice the regulator usually has subtle and maybe not-so-subtle ways to apply pressure, making it difficult for organizations to disregard them with complete impunity.

The legislators have a tough time to write laws in such a way that even organizations who keep strictly to the letter of the law, doing just the bare minimum, are still going to be protecting information adequately, yet at the same time giving proactive organizations some latitude to interpret the legal requirements more creatively in their own circumstances, particularly where this increases security. There is an art to this.

As a general rule, laws and regulations are considered something of a last resort, of benefit only where self-regulation has patently failed. This tends to happen in situations where the interests of organizations (for example, to make a profit) conflict with those of, say, its employees, customers, the general public or the state. These frameworks therefore tend to be piecemeal, focusing on specific security topics (such as confidentiality, in general) and ignoring many others (such as availability).

## The drawbacks of security frameworks

Unfortunately, while security frameworks can provide you with some help and value, all of them have drawbacks or weaknesses.

### Content limitations

A weakness in most security frameworks is the narrow focus to a particular area, topic or approach. Security should be an holistic practice with input from a variety of fields and a wide-ranging overview of the problem, as well as details suitable to the situation or environment. Unfortunately, it is not easy to document such a broad approach. Some frameworks focus on the details and don't care about an overview. Some take a management view and neglect the specifics. Some focus on functional security, others on the assurance mechanisms. Everyone has a field of expertise, and that is naturally emphasized to the exclusion of other aspects.

### Define "secure" ...

As Eugene Spafford has famously said, a secure system is *one that does what it is supposed to*. Therefore, it is impossible to define a state of security that is applicable to all systems, since not all systems are, in the minds of the users, supposed to do the same thing. The individual enterprise or user must make the decision as to the type of security that is important.

This drawback runs even deeper. Security conflicts with itself in some respects. Controls enhancing confidentiality do not necessarily support integrity. The time needed to ensure data integrity and confidentiality, and the complexity these controls inevitably introduce, both impact availability.

It should, therefore, come as no surprise that one size does not fit all when it comes to security. It is inherently impossible to create a universal checklist of items which, when implemented, will *guarantee* "security." All frameworks must be assessed against your specific needs, and

implemented intelligently with regard to the local context. Even the most narrowly-scoped frameworks such as PCI-DSS are patently not 100% effective.

Is "best practice" better than "good practice"?

In the security field, we are extremely fond of the term "best practice." At face value, it sounds reasonable enough: it doesn't necessarily imply that something is perfect but it does support the idea that we are doing the finest job we can in a real and, frankly, flawed world.

Unfortunately, we don't stop to think what that really means.

Does best practice mean something that will work for everyone in all situations? We have already determined that there is very little (possibly nothing) that will be "secure" in any and every environment – the security controls need to reflect the specific risks. Does best practice mean a minimum level of security required by all? Does it mean an optimal balance? We don't know. There is no agreed upon definition of "best practice." Although it sounds great, the term is close to meaningless. Probably the closest we can come to defining the term in any useful way is to say that it refers to activities or processes that a number of experienced people agree are useful or helpful in improving security in common situations.

Unfortunately, a number of security frameworks have, themselves, fallen into this trap. Describing themselves as "best practice," they have failed to define what this actually means to those who would use them. Examine such claims cynically.

By the way, using "good practice" instead is really just a cop-out. The issues are the same.

### Accountability

Being held to account by some authority figure for non-compliance with an obligation is only a drawback as far as the guilty are concerned! To the authority, stakeholders and other interested bystanders, accountability is an important benefit of mandatory security frameworks. The threat of sanctions such as prosecution, fines and jail sentences works as a deterrent control, pressuring organizations and individuals into complying with and fulfilling their obligations.

Note that accountability is markedly different to responsibility. Whereas people further down a chain of command may be made responsible by management for doing certain things, those at the top generally carry the can as far as accountability goes – it's a sticky attribute. That said, we are all personally accountable for our own actions and inactions.

### Responsibilities for enforcement and compliance

Broadly speaking, 'the authorities' are responsible for ensuring and enforcing compliance with laws and regulations. They simply do not have the resources to investigate and prosecute all infringements, however, so they are selective in which cases they take forward. Organizations or individuals can sometimes help by preparing evidence but beware: there are numerous rules, regulations and accepted practices for **forensic analysis**, governing aspects such as admissibility of evidence and chain of custody. One of the issues of interest to the judicial system is to what extent computer evidence can be trusted, and under what circumstances it has to be gathered, protected and presented: computers that have been infected by Trojan horse programs or viruses may not be under the sole control of the owner and hence some otherwise strong court cases against owners have fallen when the possibility of unauthorized remote access has been raised. As prosecution and defense lawyers, judges, expert witnesses and members of the jury all gradually become more computer literate, expect the quality and interpretation of computer evidence (especially that taken from live systems/networks, rather than simply on a hard drive or other static media) to be robustly challenged.

As stated earlier, we are all personally responsible for complying with our legal and other obligations as individuals. Managers have additional responsibilities to ensure compliance throughout the organization, with more specific legal requirements for governance falling to the Board of Directors. These obligations are fulfilled through the corporate governance framework with a comprehensive set of controls, including policies, standards, procedures, training/awareness and compliance activities.

In the case of IT-related obligations, the policies, standards, procedures and guidelines together comprising the organization's information security manual are a central part of the IT governance framework, along with the management hierarchy within IT. IT has become a pervasive element of the business and therefore many other organizational controls impact compliance with IT-related laws and regulations. The disciplinary process owned by Human Resources Department, for instance, considers serious noncompliance with information security policies *etc.* to be one of the possible reasons for summary dismissal.

All employees are expected to support and uphold the framework of information security and related controls. More than just tolerating the inconvenience of login controls, antivirus scanners and so on, proactive support means taking opportunities to impress upon colleagues the importance of compliance for their own good as well as for the organization and even society as a whole.

Compliance activities include:

- Awareness, training and educational activities (such as this briefing!) to ensure that everyone understands their obligations in respect of information security *etc.*;
- Periodic/regular reviews, checks and audits on the operation of the controls, including technical, procedural and managerial controls, both internally (within the organization) and in some cases externally (*e.g.* confirming that third parties are complying with their contract or license terms);
- Ad-hoc/unannounced checks, not to 'catch people out' as the paranoid might believe but to fill in the gaps between scheduled reviews, focusing on specific problem areas or perceived high risks and responding to actual incidents and near-misses;
- Structured, formalized management processes for confirming and dealing with identified noncompliance, plus informal processes such as 'off-the-record' reminders to staff about protecting sensitive or valuable information;
- Legal action, generally as a last resort. This is an expensive option that cannot easily be dropped or reversed once started. Professional, qualified legal advice is essential, ideally well in advance.

## Evidence gathering, prosecution and jurisdiction issues

Imagine a typical hacking scenario: a Ukrainian hacker secretly routes his attack through 'stepping stone' servers in Portugal and the Bahamas to attack the target system, an Australian bank's Web server hosted in Texas, USA. The hacker may be breaking the laws of any of those five countries named, and indeed others too since the Internet traffic traverses many other countries. Most of the bank's customers may be Australian citizens but some will be foreigners. If the hacker compromises the bank account of, say, an Indonesian customer who is understandably upset at the privacy lapse, what action can be taken and under whose jurisdiction? There is no easy answer, other than 'consult a lawyer', and even they tend to consult learned colleagues on complex matters such as this.

Even gathering information to make a case can be frustrated by the flow of information across borders, along with differing legal and regulatory obligations, constraints and interpretations. Legitimate investigation in one country may be viewed as illegal wiretapping or a privacy breach in another. On top of that, international criminal gangs have the funding, motivation and skills to use concealment techniques, ranging from registering phishing site domains under false identities and

stolen credit cards, perhaps using black market Internet Service Providers offering client anonymity as part of their package, to the use of 'tor'/onion routing using anonymous proxies to relay and obscure the origin of Internet traffic. Money laundering schemes using naïve and/or greedy "money mules", stolen online auction user IDs and (for example) Western Union cash drops are common. Such schemes existed pre-Internet but now international recruitment is much easier thanks to spam emails and misleading websites.

## Compliance risks, costs and benefits

Failure to comply fully with applicable laws and regulations creates risks to the organization as a whole, its officers/executive managers personally, other stakeholders including employees, and to the 'data subjects' (for personal information) and other owners or originators of information in its care:

- The organization may be prosecuted, fined or otherwise sanctioned for noncompliance. It may be prevented from doing business through the withdrawal of essential operating licenses. Bad publicity arising from compliance failures and security incidents harms the organization's reputation, hurting the bottom line through customer defections and price pressures.
- Officers, directors *etc.* may be prosecuted, fined, jailed and/or fired if they are judged personally liable for compliance failures. As well as management, other stakeholders (shareholders, employees, business partners ...) are likely to suffer indirectly from the adverse publicity.
- Employees directly involved or implicated in security breaches and noncompliance with applicable laws and regulations are likely to face disciplinary action and/or prosecution. Such incidents are hardly career-enhancing! In a wider sense, all employees suffer if the organization's profits or share price are damaged as a result of a noncompliance incident, and even more generally if the organization suffers security breaches as a result of failing to implement recommended security practices. It's a simple piece of economics.
- Data subjects, users and/or owners suffer if confidentiality, integrity and/or availability of information are compromised. Unauthorized disclosure of personal, corporate or national secrets is an obvious breach but so too is inaccurate or incomplete data (e.g. acceptance of false credentials as in identity theft) and deletion/damage or denial of access to essential information (e.g. in a denial-of-service attack on, say, a stock exchange or medical system).

## Conclusion

Information security compliance is an important executive-level corporate governance issue, and supports the organization's management of risks. Ideally, executive management should provide an annual compliance report to the Board of Directors, clarifying the overall status of the organization's information security program in relation to applicable laws, regulations, standards and policies. Given the legal and commercial issues and obvious complexities in this area (as indicated by the length of this high-level security awareness briefing!), someone senior should be tasked with ensuring that employees are well aware their security compliance responsibilities and actually fulfill their obligations. Accountability is key!

## More information and references

Please contact the CIO, the Information Security Manager, Legal or HR Departments or other qualified experts for more information and advice on security compliance. The Security Zone, Information Security's intranet area, contains other resources and the [NoticeBored security compliance links collection](#) has hyperlinks to further Web sources.

An accompanying paper outlines security frameworks 'from Audit to Zachman'.



### Important note from IsecT Ltd.

This generic document was originally delivered as part of our information security awareness service, [NoticeBored](#). We gratefully acknowledge the valuable contribution of Rob Slade.

Because it is generic, this paper cannot fully reflect every reader's situation. It may be inappropriate, inaccurate or incomplete as far as your organization is concerned because we are not familiar with your organization's specific circumstances or information security needs. It is certainly *not* legal advice. Consult a qualified lawyer for that.



This work is copyright © 2011, [IsecT Ltd.](#), 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 it is:

- (a) Not published in any public forum other than those explicitly authorized for this purpose by IsecT Ltd.;
- (b) Not sold or incorporated into a commercial product; and
- (c) Properly attributed to IsecT Ltd.

# NOTICEBORED

Read all about our information security awareness subscription service at [www.NoticeBored.com](http://www.NoticeBored.com)