

# Information security frameworks from "Audit" to "Zachman"

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

## Executive summary

Despite its length, this paper is at best a superficial introduction to information security frameworks, covering security standards, laws, regulations and security recommendations or obligations of various kinds. Our aim is not to line you up to pass a professional examination in this area, but rather to illustrate the breadth of the field and perhaps open your eyes to new possibilities and maybe prompt you to explore the most relevant aspects in more detail later. Even a quick skim through the pages that follow will give you an enormous clue as to why 'everyone is always going on about security compliance'. We may not literally cover every letter from A to Z, but its close.

## 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 lately it has become 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. Some frameworks are only peripherally related but have come to be seen as having a bearing on IT, systems and/or information security. Various financial services frameworks, laws, instructions and standards, for instance, 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.

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 and information-rich business processes. These have given greater urgency to the issue, pushing compliance towards the top of management's agenda. While you personally may view the incessant pressure to comply 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. Looking on the bright side, assisting with compliance takes some of the pressure off senior management who, in some cases, may end up standing in the dock in their rôle as officers of the company. Doing your best to keep the boss out of jail could be career-enhancing, just as doing the opposite may be career-limiting.

IT professionals have an important rôle to play both in informing information asset owners of their compliance obligations in technical security areas, and in promoting security best practices derived from technical standards and other security frameworks. Look through this paper to appreciate the sheer number of applicable laws, rules and regulations. Pick a standard, any applicable security standard, read it thoroughly and think about how it applies in practice to your organization. Now, who should you speak to first about compliance?

## The A to Z of information security frameworks

### Audit checklists and ICQs

A significant part of audit work involves compliance auditing, in other words assessing and comparing what is actually going on in practice in a given area against what should in theory be happening. Aside from public frameworks such as SOX, COBIT and ISO27k (see below), auditors may also be called upon to assess compliance with corporate security policies, procedures, standards and guidelines, and sometimes contractual commitments, either as a specific audit or simply in the course of routine audit assignments.

Auditors, as a breed, are comfortable if invited to determine whether the organization complies with a predefined suite of rules or obligations. If those requirements are rather narrowly and formally stated, leaving little wiggle room for interpretation or discretion, the auditors' job is relatively straightforward. In many audit assignments, however, and particularly internal audits, the auditors' brief is much less straightforward.

Checklists or **Internal Controls Questionnaires (ICQs)** are most auditors' tool of choice but don't confuse them with mere tick-lists: well-written checklists/ICQs eschew those simplistic and rather facile questions that anticipate binary yes/no answers in favor of open-ended questions that encourage the auditor to probe more deeply into each element of the scope. Even compliance audits benefit from this more intelligent form of examination, for example asking 'to what extent' a control is implemented, or 'how effective' is the control, rather than simply 'is it implemented Y/N?' Questions such as 'how' and 'when' and 'by whom' typically elucidate more revealing information, and give auditees a chance to explain why certain situations have arisen. The auditor is still left to gather and analyze the evidence before deciding whether any non-compliance is sufficiently significant ("material" in audit-speak) to report as such, or perhaps might just be quietly noted as a minor point.

Checklists/ICQs are normally written from scratch by auditors but may draw upon generic examples where appropriate. Either way, the process of deciding which aspects are important enough to be audited, and in what way they need to be checked, is arguably as valuable as the actual checklist/ICQs. It involves auditors considering the potential risks in the situation, determining (on the basis of their general knowledge or using other security frameworks for guidance) what controls would probably be appropriate and therefore ought to be present, and finally deciding how to go about substantiating the existence and effectiveness of the controls. In that sense, the checklists/ICQs are the products of bespoke virtual security frameworks conjured into being for each audit prior to the fieldwork by the auditors.

### Basel II, Basel III, GLBA and FFIEC

As should be clear to professionals in both fields, the financial services industry has very little to do with computer or information security, despite their very obvious common interest in valuable information assets. However, recent concerns in the financial world have focused government and regulatory interest in the area of internal controls and governance which has implications for those designing or reviewing information security controls and safeguards for financial systems and processes, particularly in regard to insider threats, frauds and data integrity.

**Basel** is shorthand for reports from the Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking. The banking community has its own take on risk management and, for fairly obvious reasons right now, is somewhat preoccupied with maintaining sufficient capital reserves to weather severe financial storms. This is not something IT and information security people tend to worry much about, except in as much as our life savings are withering instead of flourishing. However, the Basel accords also concern operational risk, which is more in line with the risk management that we know and love.

Recently released, **Basel III** is a somewhat belated response to the current global economic meltdown that **Basel II** was *supposed* to forestall. What effect Basel III will have on operational and information risks has yet to be determined.

The Financial Services Modernization or **Gramm-Leach-Bliley Act (GLBA)** [USA] concerns the privacy and security of financial information. It effectively mandates the use of risk assessment by banks to derive their specific control requirements.

The **Federal Financial Institutions Examination Council (FFIEC)** [USA] promotes and coordinates compliance with banking industry regulations. Their 405-page Banking Secrecy Act/Anti Money Laundering Examination Manual lays out the compliance expectations, guiding examiners/auditors carrying out BSA/AML and **Office of Foreign Assets Control (OFAC)** examinations/audits. Their IT Examination Handbook requires financial institutions' security controls to be based on a sound analysis of risks – that's sound as in well founded and reasonably complete, not loud.

### BSC

The elegant, some would say deceptively simple, **Balanced Scorecard** concept was introduced to an eager business world in the early 1990s by Kaplan and Norton through the Harvard Business Review. It is essentially a metrics and management reporting tool or approach, concerned with measurement-based management.

The "balanced" part is a reminder to view businesses from multiple perspectives without over-emphasizing the traditional financial measures and neglecting other important facets. Specifically, drawing up a BSC as originally described involves setting objectives and measuring performance across the four distinct domains of:

- Learning and growth (employee training and development);
- (Internal) business processes;
- Customer (satisfaction and product quality); and
- Financial perspectives.

While these four domains were chosen and defined quite specifically by Kaplan and Norton on the basis of their original research and insight, some organizations have developed their own variant scorecards based on some other selection of four parameters, arguably because they fit so conveniently into the dreaded two-by-two matrix so beloved of certain management consultants. That notwithstanding, BSC remains a worthwhile approach to establish meaningful, practical and well-rounded security metrics, mitigating some of the risks of creating biased and unrealistic metrics or measurement baselines.

For a graphical view of BSC, see [www.balancedscorecard.org/basics/bsc1.html](http://www.balancedscorecard.org/basics/bsc1.html)

### Calder-Moir IT Governance Framework

Supposedly in order to help you get the various security frameworks to work together harmoniously, the Calder-Moir IT Governance Framework is really only a graphical representation or classification of the various frameworks according to whether they address the topics of business strategy, business and risk environment, IT strategy, operations, capabilities or change management. Judge its value for yourself at [www.itgovernance.co.uk/page.framework](http://www.itgovernance.co.uk/page.framework).

### COBIT

Widely used and, until the rise ISO27k at least, probably the most recognized of the security frameworks, **COBIT** is directed at information security. However, it should be noted that COBIT was created by a specific group for a specific purpose.

COBIT was created by ISACA, originally the Information Systems Audit and Control Association. Auditability is key to COBIT and the accounting and management background definitely shows in

the choice of items in the COBIT framework. Much of the activity suggested relates to measurement, performance and reporting. Thus, in a sense, most of COBIT concentrates on what can be counted and demonstrated, arguably sometimes disregarding what might actually be effective.

If you work through COBIT you will, in fact, note that it says almost nothing at all about information technology or security *per se*. This is definitely a non-technical framework.

COBIT breaks the list of suggested controls into four phases or domains, dealing with "Planning and Organization," "Acquisition and Implementation," "Delivery and Support," and "Monitoring." (It is not too much of a stretch to see the Deming PDCA cycle in this structure as well. In fact, a great many process-based frameworks demonstrate the subtle influence of Deming's ground-breaking approach to quality management). The checklist of controls is extensive and a valuable tool to ensure that no major area is neglected. COBIT is well suited to organizations that

are primarily concerned about issues of compliance (for example, under SOX): the emphasis on audit provides a good way to demonstrate or prove the existence of controls of many types.

COBIT is not, however, confined to information security and addresses a large number of other areas. Therefore, basing a security review on COBIT may require extensive resources and will definitely demand activity from areas of the enterprise outside of the information security department.

## Common Criteria

Contrary to much mistaken opinion, the **Common Criteria (CC)**, more properly the Common Criteria for Information Technology Security Evaluation, and also ISO 15408) is not a security framework or standard of practice. It isn't even a methodology for evaluating security products or systems. CC is a structure for specifying product and product evaluation standards.

The basic result of following the CC structure is the production of a **Protection Profile (PP)**. A PP outlines a general class of security devices or products, describing the environment within which such an entity is expected to work, and the security functions that should be implemented. The part of the PP that can be used to evaluate a specific device is known as the **Security Target (ST)**. Evaluations of products against STs are done on the basis of seven levels of increasing confidence in the assessment, the **Evaluation Assurance Levels** (yes - you guessed it - **EALs**).

At the moment, [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org) seems to be a reliable source of information about CC.

There are generally three parts, or documents, related to the CC overall. **Part One** is a general

### What's in a name?

The capitalization of COBIT varies: some use COBIT, COBiT, CObIT, and CobiT, while ISACA itself prefers COBIT with the middle capitals in a smaller font size. There are even variations on the expansion of the acronym. COBIT originally meant **Control Objectives for Information Technology**. This was subsequently expanded to cover "Information and Related Technologies" but ISACA's current literature seldom even mentions the expansion at all. In the same way that ISACA dropped the acronym for its own name and prefers to be known solely by its initials, COBIT is now the preferred name.

### CCcompliance

It is not enough to know that a product has "passed" the Common Criteria. In order to understand what that might imply, the details of the PP, ST, and EAL must be known as well. As those who have dealt with ISO 9000, the standard on quality, are aware, it is perfectly possible to document your quality standards and procedures in a manner consistent with the ISO 9000 requirements, and still have them say no more than "we make consistently lousy products." In the same way, it is possible to be CC "compliant" with a certification that says "the product provides almost no protection, and we're only judging that based on hearsay."

introduction, outlining the basic ideas and major terminology used. The Part One document isn't hard to read and probably every security professional should have read through it at least once. **Part Two** addresses functional security, the aspects that we normally consider to be security technologies and activities. This document stipulates how to express the requirements for functional security for a particular device. Outside of developers or evaluators working with or towards an evaluation, Part Two is not something you will want to plow through, unless you have serious problems with insomnia. **Part Three** deals with assurance: the question of how we know that the functional security is actually providing the protection that we want it to provide. Like Part Two it sets forth the language and format for requirements and specifications, and the document is even longer. However, this part also contains an overview of the seven EALs. While the text is not exactly easy to work through, this section of the CC is one with which more security professionals should be familiar.

### Contractual commitments

Well-written and properly executed contracts and agreements carry the force of law and hence compliance is mandatory, in theory if not always in practice. Therein lies the rub.

**Employment contracts** and/or the accompanying Codes of Conduct, Employee Manuals, Employment Guidelines, Company Rulebooks *etc.* (which may be explicitly referenced by the employment contracts) usually impose obligations on employees in respect of confidentiality of information belonging to their employer and some call out obligations to secure private information provided by customers *etc.*

**Non Disclosure Agreements (NDAs)** or confidentiality agreements typically oblige the signatories not to disclose information supplied in connection with a project *etc.* that a reasonable person would accept as being confidential, and which has not already been disclosed by the owner or some third party.

### COSO

... is shorthand for the **Committee of Sponsoring Organizations** of the Treadway Commission, Enterprise Risk Management Integrated Framework. The Treadway Commission was established, in the United States to address a fear (subsequent to some major financial failures) that small investors would lose faith in the stock markets and, in particular, in the financial reports from publicly-traded companies. As such, COSO seeks to ensure that there are internal controls to enhance the reliability of public disclosures. Like COBIT, COSO is primarily concerned with internal controls and audit. In contrast to COBIT, which concentrates on IT, COSO is concerned with business risk of which IT risk is just one facet.

COSO outlines a three dimensional or cubic framework for examining controls. On one axis are four categories of objectives: strategic, operations, reporting, and compliance. A second axis lists four unit-levels of an enterprise: entity-level, division, business unit, and subsidiary. The final face of the cube has eight components of risk management: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Again, while COSO provides a framework for examining a number of aspects of the business, it does not provide any explicit list of controls, practices or methodologies.

### Digisigs

**Digital signatures** are gradually being accepted by the courts as legally binding through the introduction of laws and regulations worldwide. The Food and Drug Administration's **21 CFR Part 11 – Electronic Records; Electronic Signatures [USA]** is but one example, laying out the terms and conditions under which the FDA will accept electronic signatures.

## Email security laws

Ordinary advertisements, mailshots *etc.* are covered by traditional laws against fraud, misleading claims *etc.* Additional legislation has been introduced in many places to cover the worst excesses of modern IT-enabled high pressure marketing and sales techniques, particularly spam (unsolicited commercial email, usually sent in bulk).

Controlling the **Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM)** [USA] permits organizations to send unsolicited commercial email provided it contains an opt-out mechanism, a valid subject line and header, the legitimate physical address of the mailer and a label if the content is adult. Organizations are free to email existing customers or other parties with whom they have prior relationships.

Under the **Unsolicited Electronic Messages Act** [NZ], recipients must consent (opt-in) to receiving promotional emails. Consequently, we Kiwis have no need for anti-spam software since our in-boxes are totally uncluttered [/wishful-thinking].

## FISMA

The **Federal Information Systems Management Act (FISMA)** [USA] mandates certain standards of information security and controls for US federal agencies. It extends to contractors and other sources that support the assets of federal government departments. Aside from the formal scope, however, FISMA potentially has wider application. It provides a solid basis for security management, assessment and assurance for large corporations as well.

Specifics on the implementation of FISMA vary somewhat. The legislation states that standards must be applied but the standards are different for different agencies and applications. Detailed instructions can be found in directives for the military (Defense Information Technology Systems Certification and Accreditation Process - DITSCAP), the intelligence community (Director of Central Intelligence Directive 6/3 or DCID 6/3), and more generally the National Information Assurance Certification and Accreditation Process (NIACAP). The National Institute of Standards and Technology also has outlines (see the later section on NIST standards for details of this and other documents).

## FOIA

**Freedom Of Information Acts (FOIA)** [USA, UK *etc.*] go against the grain of most other information-related legislation in that they force limited disclosure of certain information by public bodies where this is in the public interest. Problems can occur with information that was provided in confidence such as commercially-sensitive pricing information within tender documents and contracts, and personal identity information provided to access many public services. Tensions between FOIA and privacy/commercial confidentiality laws seem likely to remain indefinitely.

## Fraud and forgery/counterfeiting laws

Most countries have laws against fraud, theft by deception and similar criminal acts. The Financial Management and Accountability Act [Australia] mandates a fraud control plan for government agencies, among other things. Section **419** of the Nigerian Penal Code is perhaps the most famous, though probably the least effective, anti-fraud laws. It is *supposed* to curb advance fee frauds originating in Nigeria. We can but wonder at how many Nigerian frauds there might have been *without* section 419! Mind you, some '419 scammers' live in other West African countries and the criminal gangs behind them have set up remote operations in London, Amsterdam and elsewhere, so the Nigerian legislature is not entirely to blame.

Identity theft laws are gradually creeping into the statute books. Stealing a person's identity is a particularly worrisome crime for the individual victim and is increasingly of concern to society as a

whole. So many official processes rely on a person's identity that widespread identity theft threatens the very basis of the social security, healthcare, tax and even criminal justice systems.

## GAISP

Nothing much has been heard from the project team developing the **Generally Accepted Information Security Principles (GAISP)** since 2003, when v3.0 was released. GAISP evolved from an earlier project, **Generally Accepted System Security Practices (GASSP)**, which itself stemmed from US government interest in defining a security framework of baseline IT security controls back in the early 1990s.

The project was basically building a repository of commonly-used information security controls. It's a shame that the project petered out despite being taken on by the **Information Systems Security Association (ISSA)**, leaving us to speculate on its demise: possibly they found it difficult to agree on a comprehensive baseline that was universally applicable, or perhaps the project was overtaken by ISO27k and other frameworks noted here. More prosaically, it could simply be that the project team got bored – who knows? Anyway, v3.0 seems destined to be the last GASSP.

## GAIT

**Guide to the Assessment of IT risk (GAIT)** is the Institute of Internal Auditors' top-down method or framework to identify key IT risks such as SOX-relevant IT-related risks that could materially impact the financial statements, and those covered by PCI-DSS, HIPAA *etc.* and to assess the associated IT controls within the organization. Unfortunately, though, it is only available to IIA members ☹

## Hacking, wiretapping and information security laws

Unauthorized logical access to computer networks, systems and data ("hacking") creates problems for the legislatures in many countries. The physical equivalent known as "trespass" is usually only treated as a minor crime and normally requires the victim to have taken reasonable measures to secure/protect their property. Through laws such as **Computer Misuse Act (CMA)** [UK] and **Computer Fraud and Abuse Act (CFAA)** [USA], legislators have found it difficult to define terms such as "unauthorized access" and "reasonable measures" in the context of IT. Furthermore, there may be no tangible evidence that someone has hacked a networked system yet the impacts can be dramatic.

Wiretapping or interception of private data communications, phone calls, emails *etc.* is permitted for certain limited law-enforcement or national security purposes but is otherwise prohibited through laws such as the **Telecommunications Act** [Australia] and **Crime Control and Safe Streets Act** [USA]. Not even US Presidents are above the law on wiretaps – remember Watergate? Unauthorized interception of wireless network signals may fall foul of longstanding legislation governing the use of radios by private citizens in some countries.

## Industry regulations and professional rules of conduct

In addition to laws, a number of para-legal rules and regulations affect IT and information use in particular industries and professions. Most are mandated by government-appointed industry regulators, some by associations promoting professional standards and ethics among their members. In many respects, compliance with such rules and regulations is as important as legal compliance since noncompliance can result in heavy sanctions (such as withdrawing a license necessary to conduct business) and may be used as evidence supporting a legal challenge. [Not being totally familiar with your industry, we won't actually name any, but your senior management, compliance people and auditors probably know what we're on about.]

## IPR

Laws in most countries provide legal protection for the owners of intellectual property (hence **Intellectual Property Rights, IPR**) including computer data, software and information in whatever medium. Terms such as 'ownership' and 'intellectual property' are quite tricky to define in law, thus contributing to extensive differences in the small print and legal status of **copyright** (e.g. software licenses), **patents**, **trademarks** and **designs** around the World. Global harmonization is happening slowly, two specific examples being (a) the gradual move away from the need to "register" copyright with the authorities, and (b) pressure to widen the use of patents to protect proprietary business processes and the associated software systems, outside of the US.

Unauthorized copying, dissemination or use of licensed software is known as piracy. Piracy is very much a global problem and is barely under control anywhere. Western news media are fond of highlighting a 'total disregard' for copyright in the Far East, citing the occasional discovery of factories churning out millions of counterfeit CD-ROMs complete with authentic-looking holographic panels. A simple comparison of the number of licensed products sold against the number of computer systems reveals the truth that piracy is rife in the West too. Prosecutions under the **Digital Millennium Copyright Act (DMCA)** [USA] and similar laws worldwide have fired warning shots across the bows of anyone intent on copying and communicating music and video files through peer to peer file sharing. Software industry bodies such as the BSA (Business Software Alliance) have had a few notable successes in prosecuting pirates, most notably a penalty of well over half a million dollars for one company coming on top of the internal costs to clean up their act.

Laws such as the **Economic Espionage Act (EEA)** [USA] protect proprietary information (trade secrets) from unauthorized disclosure and use. Although a lot of such information exists as computer data these days, the laws cover proprietary information in any format.

## ISF

The Information Security Forum's **Standard of Good Practice for Information Security** is a guideline forming a checklist of policies or attitudes towards information that the organization and its employees should have. It is structured in five "aspects": Security Management, Critical Business Applications, Computer Installations, Networks, Systems and Development. These aspects are broken out into 30 "areas," and the areas into 135 "sections" (there's that magic number again).

Within Security Management, the areas are high-level direction, security organization, security requirements, secure environment, malicious attack, special topics, and management review. For Critical Business Applications there are security requirements, application management, user environment, system management, local security management, and special topics. Computer Installations involve installation management, live environment, system operation, access control, local security management, and service continuity. Networks require network management, traffic management, network operations, local security management, and voice networks. For Systems Development pay attention to development management, local security management, business requirements, design and build, testing, and implementation.

The 135 sections do not all have equal levels of detail. Management, for example, gets much more attention and material. The first section (of three) from "High-level direction" (Section SM1.1) deals with management commitment. It sets out the principle that senior management's direction on information security should be established, and commitment demonstrated. The objective is to establish top management's direction on, and commitment to, information security. It goes on to note that board-level executives or the equivalent should have a high level of commitment to achieving high standards of corporate governance, such as those required by various national standards, treating information security as a critical business issue, creating a security-positive environment, and demonstrating to third parties that the enterprise deals with information security in a professional manner. Top management should have a high level of commitment to applying fundamental principles, for example, assuming ultimate responsibility for the internal controls of the

enterprise, ensuring that controls over information and systems are proportional to risk assessed, assigning responsibility for identifying, classifying and safeguarding information and systems to system owners, granting access to information and systems in accordance with explicit criteria (policy). Management should demonstrate their commitment to information security by setting direction for information security (in policy), assigning overall responsibility for information security to a top-level director or equivalent, chairing key information security working groups, monitoring the security condition of the enterprise, and allocating sufficient resources to information security.

Unfortunately, a later section on malicious mobile code simply states that there should be a means of dealing with it, and lists some risk factors.

The ISF standard is, however, one of few frameworks available without charge. The ~250 page document provides useful advice in a number of areas after the promotional early parts. It can be downloaded from the [ISF website](#) or directly from [www.isfsecuritystandard.com](http://www.isfsecuritystandard.com).

### ISM<sup>3</sup>

The Information **Security Management Maturity Model (ISM<sup>3</sup>, ISM<sup>3</sup> or ISM-cubed)** is an interesting blend, consisting of a kind of superset or integration of other security frameworks such as ISO27k and SSE-CMM. ISM<sup>3</sup> was developed and promoted by a consortium of information security consultancies providing ISM<sup>3</sup> training courses. ISM<sup>3</sup> itself has been slowly maturing for several years but according to the ISM<sup>3</sup> website [www.ISM3.com](http://www.ISM3.com), it is about to be published by The Open Group and is not currently available ☹

### ISO27k and other ISO standards

As noted earlier, **ISO27k** (*i.e.* the **ISO/IEC 27000-series** information security standards) is a particular favorite of ours. We make no apology for this: ISO27k has become the leading - as in most widely used – international standard for information security with nearly 7,000 organizations certified compliant with ISO/IEC 27001 and many many more using the standards without being formally certified.

Note that ISO27k explicitly concerns *information* security, not just *IT* security. While the vast bulk of information these days is computerized, the security principles and controls also apply to information in other forms such as on paper or in people's heads (knowledge, experience, expertise and skills). Physical and procedural/administrative controls are every bit as important as logical/system controls.

The first two ISO27k standards were derived directly from British Standard BS7799, published back in 1995. BS7799 owed its existence to an even earlier security policy manual from an oil company and, as such, was already somewhat outdated at the time it was adopted first by the British Standards Institute and then by ISO/IEC. It didn't mention the Internet, for example, and was biased towards organizations using mainframes under central control. The ISO27k standards are being updated but as it normally takes two years or more to prepare, agree and release each standard or update, they are never really destined to be cutting edge.

Ten ISO27k standards have already been released. A dozen more are currently in preparation, expanding ISO27k to cover specialty areas, provide industry-specific implementation guidelines *etc.* Rather than boring you stiff by covering *all* the ISO27k standards here, we outline four key ISO27k standards below but please refer to either the ISO site [www.ISO.org](http://www.ISO.org) or to [www.ISO27001security.com](http://www.ISO27001security.com) for the full nine yards.

We should mention that there are lots more ISO and ISO/IEC standards, some of which cover information security, IT security, physical security, risk management and other topics. Read about them at <http://www.iso27001security.com/html/others.html#ISOstds>.

## ISO/IEC 27000

ISO/IEC 27000 provides an introductory overview or guide to the entire ISO27k family, plus a succinct glossary formally defining certain specific information security terms as they are used throughout ISO27k. This is a useful standard in its own right and, best of all, it is available [free of charge!](#)

## ISO/IEC 27001

Part 2 of BS7799, first published in 1999, introduced the concept of an **Information Security Management System (ISMS)**, in other words a structured and systematic way for management to direct and control its information security activities. This became ISO/IEC 27001 in 2005.

ISO/IEC 27001 is a formal specification standard, meaning that organizations can choose to be formally assessed by accredited certification bodies to determine whether they fully comply with the management system it describes, gaining an ISO/IEC 27001 compliance certificate if (or more usually when) they pass.

The management system described in ISO/IEC 27001 embodies Edward Deming's well-known **PDCA cycle (Plan → Do → Check → Act)**. In summary:

- **Plan** means determine what information assets deserve protection, to what extent and how by assessing information security risks;
- **Do** means implement appropriate risk treatments, mostly being information security controls such as those described in ISO/IEC 27002;
- **Check** means periodically review the security status to determine whether the desired level of protection has in fact been achieved, and to take account of any changes in the information assets, information security risks *etc.*;
- **Act** means take corrective action to maintain alignment between the desired and actual levels of security, if necessary going back to the planning and doing phases for major re-work.

## ISO/IEC 27002

ISO/IEC 27002, derived from part 1 of BS7799 and originally numbered ISO/IEC 17799, is one of the earliest frameworks specifically addressing information security and is probably the most important and widely used. It is of significant interest to the information security community world-wide and is coming to the attention of governments, legislators and regulators writing information security and privacy-related laws and regulations.

Although ISO/IEC 27002 does not provide explicit technical or implementation details, it describes in general terms a reasonably comprehensive suite of information security controls categorized into 11 broad-brush areas (called clauses) including:

- Security policies
- HR practices such as security awareness
- Physical protection of IT facilities
- IT computer and network operations
- Security in software development
- Contingency planning
- Compliance ... *etc.*

### Is 135 a magic number?

There seems to be something magical about 135 in relation to security. An astounding number of the security frameworks have roughly 135 controls, objectives or questions. The number of security frameworks is not far off 135. When you go to purchase the various documents, you'll need to find approximately U\$135 for most of them, regardless of their size or complexity...

The 11 clauses are surprisingly similar to the 10 domains of (ISC)<sup>2</sup>'s Common Body of Knowledge (CBK). Within the 11 clauses, it lays out 33 carefully-worded "control objectives" (*i.e.* what the controls are anticipated to achieve for the organization), followed by textual descriptions of typical controls that should be considered under 133 subheadings.

Note that ISO/IEC 27002 does not actually mandate *any* controls as such but leaves those crucial decisions to management of the organizations that adopt the framework. This is quite deliberate since each organization has its own unique situation, facing a particular combination of information security risks and all manner of constraints. Even strategic and commercial objectives play their part in determining the organization's "risk appetite". In practice, controls such as antivirus, user logins and data backups are almost universal but even these might not be appropriate in some conceivable situations.

### ISO/IEC 27005

ISO/IEC 27005 is an information security risk management standard which is important because ISO27k is predicated on a risk-based approach. Essentially, organizations are encouraged to identify and address the greatest information security risks first, then cycle repeatedly back through the risk analysis and risk treatment activities addressing progressively smaller risks plus any that have come to the fore since the previous cycle. It's a kind of whack-a-mole game that links in neatly to the Deming PDCA cycle. However, the current immaturity of the field of information security risk management means that it is more art than science. ISO/IEC 27005 does not mandate a particular information security risk analysis, assessment or management process, rather it provides general guidance on how to select and apply one or more methods to suit the organization's purposes.

### IT and information security standards

There is an enormous range of publicly-available IT and information security standards covering, for example, the technical aspects of data communications protocols and encryption schemes, as well as more general ones such as ISO27k and ITIL. Compliance with standards is (usually) optional. An organization may readily develop and sell proprietary (nonstandard) networking and encryption products, for example, although their target markets are likely to be constrained due to customer demands for standardization, particularly in terms of interoperability and avoiding vendor lock-in. On the other hand, some standards are linked to, and effectively mandated by, laws or regulations, whether explicitly or by inference and practice. Privacy laws in Japan, for example, leave Japanese organizations little option but to implement ISO/IEC 27002.

### IT-Grundschutz

Since 1994, BSI (no, not the British Standards Institute this time but **B**undesamt fur **S**icherheit in der **I**nformationstechnik - the German federal government office for information security) has published and maintained the **IT-Grundschutz** (IT baseline protection) manual. The manual describes a security framework comprising a governance structure plus a comprehensive suite of information security controls ranging from technological, organizational and sociological to infrastructural (physical) in nature. It has now been divided to separate the methods (which are gradually being aligned with ISO27k) from a huge catalog of threats and controls. There are some oddities as a consequence of shoehorning the German original into the ISO27k mold, for instance noting that it uses the term "IT security" instead of "information security" because it is equivalent but shorter - in fact, these are subtly different concepts. The main difference is that IT-Grundschutz recommends the adoption of a standardized *de facto* security baseline as a starting point rather than ISO27k's pure *de novo* risk-based approach. Both have their merits.

### ITIL and ISO 20000

The **I**nformation **T**echnology **I**nfrasturcture **L**ibrary (**ITIL**) is a massive, rather pricy set of documentation and training courses aimed at improving information technology service management. It was originally prepared for the British Government and still has vague overtones of *Yes, Prime Minister*, being somewhat bureaucratic and overbearing for lean and mean private

sector enterprises. Even though ITIL may or may not address information security specifically (they keep changing their minds about including that section!), proper management generally leads to and supports better security, so it fairly naturally follows that this library of practices would be of interest to information security professionals.

**ISO 20000** is an international standard based on ITIL but there has been an interesting fork in the road since it was created. Development of ITIL and ISO 20000 continue but now along separate paths.

### National security and anti-terrorism laws

In matters of national security and terrorism, the normal checks and balances preventing authorities from prying into the affairs of their citizens and foreigners are substantially moderated if not completely suspended. The situation changed substantially after 9/11 with many government agencies gaining far more wide-ranging powers in order to tackle terrorism and organized crime. The **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT)** [USA] is an example which modified previous laws such as **Foreign Intelligence Surveillance Act (FISA)** and **Electronic Communications Privacy Act (ECPA)**, creating civil liberties issues.

One way the authorities tackle terrorism is by going after their finances. The **Money Laundering Control Act** [USA] and similar laws elsewhere aim to bring traceability and accountability to the global flows of money (covering not just hard cash but electronic transfers also).

The **Official Secrets Acts** [most countries] typically specify draconian measures to ensure secrecy of information relating to protection of the realm, with harsh penalties up to and sometimes including death for spies and other traitors. Strong encryption (*i.e.* particular encryption algorithms and/or long keys) is sometimes treated as munitions with restrictions on exports of the associated software, hardware and documentation.

### NFPA 1600 and BS25999

Conceptually speaking, business continuity encompasses *both*:

- Resilience and capacity measures, along with preventive controls, to ensure the reliable operation of vital business processes and, of course, the supporting infrastructure including critical IT systems and networks despite most run-of-the-mill security incidents; *plus*
- Plans, procedures and other detective and corrective controls to aide rapid and efficient recovery from more significant disasters that overwhelm or undermine the preventive controls.

The intimate relationship between IT and The Business makes this an ideal area for collaboration through a jointly understood framework.

The US **National Fire Protection Association (NFPA)** standard **1600** on Disaster/Emergency Management and Business Continuity Programs, promotes a governance framework and overall approach to managing disasters, such as serious information security incidents.

**British Standard BS25999** on **Business Continuity Management (BCM)** is similar to BS7799 in that it consists of two complementary parts: (1) a 'code of practice' offering implementation guidance plus a set of best practice BCM controls covering the whole BCM lifecycle; and (2) a formal specification for a business continuity management system against which organizations may potentially be certified compliant.

### NIST SP800s

It really isn't fair to compare the **Computer Security Resource Center (CSRC)** of the US **National Institute of Standards and Technology (NIST)** with the security frameworks we have been discussing. Even though it is only one office of the institute, CSRC is known simply as NIST in the security community. It provides a wealth of well-written, often highly detailed information,

standards and related resources in a wide variety of information security topics, which are freely available from <http://csrc.nist.gov>. The publications section is particularly useful, with a constantly updated stream of guidelines and aids, particularly the **Special Publications 800-series (SP800)** documents. Americans should use them since this is what your tax dollars have bought. Everybody else might as well use them too since the Americans have already paid the price, and to be honest, they are extremely good.

### OCTAVE and 77 other risk management methods

The **Operationally Critical Threat, Asset, and Vulnerability Evaluation** process (**OCTAVE**) is not really a security framework as such but a risk management method from Carnegie Mellon University. This formal and detailed set of processes assists in ensuring that risks are identified and properly analyzed, following the standard techniques used in most risk analysis procedures. However, due to the level of activity and overhead involved in OCTAVE, it is probably best suited to large organizations or projects. The OCTAVE group has tacitly admitted this recently with a modified version for smaller businesses.

For an outline of some 78 (!) information security risk analysis, risk assessment and risk management support tools and methods, plus hints on how to select what's best for your project, please consult the ISO27k FAQ at [www.ISO27001security.com](http://www.ISO27001security.com).

### OSSTMM

The **Open Source Security Testing Methodology Manual (OSSTMM)** from ISECOM [www.ISECOM.org](http://www.ISECOM.org) offers a structured approach to testing, assessing or auditing a situation to measure its security status. According to the pre-release tasters, the imminent OSSTMM version 3 framework will lead users methodically through the process of scoping the job, deepening their understanding of the situation under review and its potential weak points, and preparing for the actual testing of the security controls. OSSTMM is an open source framework in that subscribers are encouraged to contribute to its ongoing development, but it's not free.

### PCI

In response to the exploding issue of identity theft and similar card fraud, the major credit and debit card companies collaborated to release the **Payment Card Industry - Data Security Standards (PCI-DSS)**, a set of cardholder data security rules that applies to virtually any business dealing with credit card transactions. PCI-DSS is almost universally referred to simply as **PCI**, which might cause a bit of confusion for those familiar with computer bus standards.

There are four levels of PCI requirements according to the volume of transactions conducted by the business. PCI compliance is mandated through the business' contracts with their respective credit card companies, in other words this imposes a legally-binding contractual obligation towards security rather than through a general law or international standard.

The security controls in PCI are described quite explicitly, leaving little room for discretion on the part of the businesses concerned. Organizations covered by PCI need to:

- Understand their rôle in the payment system (service provider, gateway or merchant);
- Know where their card data are stored and who protects the data (e.g. any third-party service providers);
- Confirm that card data security arrangements meet the specific requirements of PCI e.g. are card data properly encrypted when stored and transmitted? Are they deleted after authorization? Are there adequate preventive (e.g. awareness/training, regular penetration tests and secure disposal of hardcopies by cross-cut shredding), detective (e.g. logging access and audit the logs for suspicious activities) and reactive/corrective controls (e.g. response

procedures)? Do employees handling card data appreciate and fulfill their obligations to maintain cardholder confidentiality?

If you deal with credit cards, you must be PCI compliant. However, there is much debate over how useful and effective PCI truly is in practice. Heartland, which suffered the largest payment card data breach in history and recently experienced yet another major loss was, on paper at least, PCI compliant both times although a Catch-22 clause means that any business that suffers a credit card incident is, by definition, non-compliant. PCI compliance does have some commercial benefits, however. It reduces the possibility of losing card data, reduces the number of opportunities for fraud, and reduces the need to report breaches. Not least, it enables the organization to process credit cards

The scope of PCI compliance is strictly limited to cardholder data, excluding other valuable and often vulnerable personal or proprietary information. This is definitely not a generally-applicable multi-purpose information security framework.

Most damagingly, some argue that PCI has hidden agenda, being a legal mechanism for the credit card companies to pass significant financial liabilities arising from information security breaches down to the merchants and banks using their cards, while at the same time protecting their own brands. It might even be said that the global credit card companies are exploiting their commercial power over the banks and merchants who are their customers. We leave it to your discretion to examine the arguments both ways.

The latest and greatest version 2 of PCI comes into force in January 2011. For details see [www.pcisecuritystandards.org/pdfs/summary\\_of\\_changes\\_highlights.pdf](http://www.pcisecuritystandards.org/pdfs/summary_of_changes_highlights.pdf).

Two other PCI security standards cover PIN entry devices and payment applications respectively.

Aside from PCI, credit card organizations need to develop and implement suitable controls in case of incidents or breaches. California **State Bill 1386 (SB 1386)**, the Security Breach Information Act [USA], forces companies whose credit card processing systems are breached to inform all the credit card holders of that fact. SB 1386 applies to any organization doing business with customers in California, while similar laws have been enacted in most US states. It supports the principle that organizations are accountable for maintaining the security of financial (and other) valuable information entrusted to them by third parties.

### Pornography laws

Definitions of pornography vary markedly around the globe. Some cultures are relatively tolerant towards sexual content and nudity that others find indecent or abhorrent. Prior to the Internet, border controls were reasonably effective at limiting the free flow of pornographic materials but, thanks to the largely unregulated Web, such tight control is no longer practicable.

There has been some success in tackling pedophilia and child abuse through widespread international cooperation but even here laws and attitudes vary between countries. The 'age of consent', for instance, is not the same everywhere.

Individuals caught at work in possession of pornographic materials, as locally defined by laws such as the **Obscene Publications Act** [UK], typically face dismissal if not prosecution and legal sanctions. Those guilty of creating, copying or distributing porn may be fined and/or jailed and, if they have been using IT/networking equipment belonging to an organization, the organization and/or its officers may perhaps be brought to account for their lax security, tolerance or even active support of the pornographers.

### Privacy laws

About half of the world has enacted legislation to protect personal privacy as a general principle. The **Information Privacy Act** [Australia], **Personal Information Protection and Electronic Documents Act (PIPEDA)** [Canada] and **Data Protection Acts (DPA)** [most European countries] for example aim to protect personal information, generally defined as information relating to

identifiable, living individuals that they would consider private and personal. Information security controls are necessary to ensure personal privacy and data integrity, including situations in which personal data are transferred abroad. In Europe, at least, the definition of personal information encompasses computer data such as personnel databases, video/CCTV and audio data, and other/hardcopy formats such as card index systems. The laws also permit people to demand copies of their personal information, primarily in order for them to be able to check the details and insist on any necessary corrections. Some personal data/privacy laws class information such as a person's sexual orientation and their criminal history as especially sensitive. Such information is obviously required for certain official, medical or other purposes but the laws aim to prevent it getting into the wrong hands.

The **Health Insurance Portability and Accountability Act (HIPAA)** [USA] concerns "individually identifiable health information". HIPAA requires security controls to protect the confidentiality, integrity and availability of all **electronic Protected Health Information (ePHI)** that the organization creates, receives, maintains or transmits. Required safeguards include appropriate policies and procedures, safeguarding physical access to ePHI and technical security measures to protect networks, computers and other electronic devices.

**FERPA (Family Education Rights and Privacy Act)** [USA] gives students rights to access educational records kept by the school, restrict disclosure of educational records, amend educational records and file complaints against the school for disclosing educational records in violation of FERPA.

Finally, the **Fair and Accurate Credit Transactions Act (FACTA)** [USA] mandates, among other things, proper disposal of credit-related information.

### SABSA

The **Sherwood Applied Business Security Architecture**, originally developed to explain the basis on which a certain security consultant worked, is in fact closely related to the Zachman framework. The SABSA site [www.sabsa.org/UserFiles/Image/2-matrix.png](http://www.sabsa.org/UserFiles/Image/2-matrix.png) also describes a process and other functions.

### Sales-related laws and regs

Laws such as the **Sale of Goods Act** [UK] and regulations from the **Federal Trade Commission (FTC)** [USA] etc. making suppliers liable for defective/non-performing goods are OK for IT hardware but rarely if ever applied to software or other information products. Warranties are expressly disclaimed by suppliers in most software licenses – and yes, software is usually licensed rather than sold. Opinions on whether this is A Good Thing depend largely on whether one's perspective is as a supplier or customer! It does seem curious that software companies can continually get away with patently defective and often insecure programs that have to be patched to perform as generally expected, yet on the other hand the market would surely resent the increased prices that would inevitably follow widespread litigation and a tightening up on software quality assurance processes. Furthermore, legal arguments about the program specifications and claimed *versus* required functionality would be horrendous, meaning extremely expensive.

### SAS 70

The **American Institute of Certified Public Accountants' (AICPA) SAS 70 (70<sup>th</sup> Statement on Auditing Standards)** is a widely used standard for structured audits of service management controls within financial services organizations, including controls for IT and related processes. SAS 70 reports by respected external auditors are often valued in dealings between financial institutions. A good SAS 70 report allegedly demonstrates that a financial services organization takes its obligations to IT security and controls seriously, although it pays to check the scope and details. **Type I** reports concern whether the organization has fairly described its controls, and

whether the controls are appropriate. **Type II** reports expand on the Type 1 content with the auditor's opinion on whether the specified controls are operating effectively, which is nice.

### "Security Governance"

Many of the security frameworks available are in the form of a checklist, so why shouldn't the "Security Governance" list from Fred Cohen's [CISO Toolkit](#) be included?

In fact, Cohen's version may be considerably easier to understand and use, particularly for those with a business, rather than a security, background. While most security frameworks are structured according to a taxonomy of security concepts, the checklist in "Security Governance" is based on business models and concepts. For example, the four major divisions are made on the basis of business functions and modeling, oversight, business risk management, and enterprise security management. Therefore, the businessperson working through the points will start with the familiar, and only later have to face items directly discussing security. (Even then, the security issues are those regarding the position and management of security within the organization.)

Regardless of other security frameworks that you may use, Cohen's checklist will be of value. While many items will have relations to details in other indices, the articles and entities in "Security Governance" address a number of issues that are not found in most security frameworks. Let's face it: regardless of the emphasis or perspective, security frameworks tend to follow the same general outline. Cohen's work is idiosyncratic--and, in this case, that's a useful characteristic.

Also, while most security frameworks give you a checklist of about 135 items for roughly \$150, Cohen gives you over 900 points for just \$49.00. Great value!

### SOX and similar laws and regs

In the wake of the Enron scandal, the **Sarbanes-Oxley Act (SOX)**, also known as **Sarbox** or more formally the Public Company Accounting Reform and Investor Protection Act [USA] emphasizes that senior management is formally accountable for the integrity (reliability, comprehensiveness, accuracy, validity ...) of financial reports about companies listed on the US stock exchange. It extends beyond that, touching on private companies doing business with other companies that provide public reports and even entities outside American jurisdiction.

SOX sections 302 and 404 (in a marvelous confusion with the common http result codes) note that the integrity of information systems and data supporting the financial reporting processes must be proactively managed and ensured by management to the satisfaction of the external auditors. To this end, auditors insist that senior managers 'attest' to the integrity of the financial reports (and hence the underlying financial data and IT systems on which they are based, plus certain elements of the general IT infrastructure and control environment), essentially placing them in the dock if the reports subsequently turn out to be pure fiction.

The **8<sup>th</sup> Directive on Company Law** [Europe] is the first pan-European analogue of SOX. Like other EU directives, this is not actually a law as such but comprises a set of guiding principles that must be incorporated into national legislation within each of the European countries in due course, gradually harmonizing all the laws in this respect. The same Europe-wide harmonization process took place for privacy/data protection during the past decade or so. Further corporate and possibly IT governance regulations are anticipated in Europe and elsewhere as this is an actively evolving field.

**Companies or Corporation Acts** [various countries] typically define the management framework for governing and controlling corporations, limited companies *etc.* The mandatory controls mostly focus on ensuring the integrity (completeness and accuracy) of financial data reported to the authorities.

The **Securities and Exchange Commission (SEC)** [USA] which oversees governance of companies listed on the US stock exchanges established the **Public Company Accounting Oversight Board (PCAOB)** to review and regulate application of SOX. The **National Association of Securities**

**Dealers (NASD) Rule 3510** [USA] requires its members to have business continuity plans plus other controls. The **Listing Rules** published by the **London Stock Exchange (LSE)**, **New York Stock Exchange (NYSE)** and **NASDAQ** (originally the **National Association of Securities Dealers Automated Quotations**) define a range of obligations for limited companies that wish their shares to be publicly traded, including those relating to the integrity of financial data reported. Similar rules are in force for other stock exchanges and markets around the world.

Accounting and auditing practices are subject to a mesh of laws and regulations. The **International Financial Reporting Standards (IFRS)** and **United States Generally Accepted Audit Practices (US GAAP)** are broadly equivalent audit/accounting standards, both of which effectively require that organization control and secure their IT systems used to generate data for financial control and reporting purposes. Data integrity (completeness, accuracy) is clearly a vital issue for corporate financial and operational data used to make important investment decisions.

### SSE-CMM

The **Systems Security Engineering - Capability Maturity Model (SSE-CMM or just CMM)**, is an attempt to apply standards of engineering rigor to information systems/IT development. The model identifies different levels of maturity of organizations in terms of their processes, documentation and disciplined approach to systems development and change management. The original model identified levels starting at informal or chaotic through repeatable, documented, managed and finally ending at continually improving. The approach has subsequently been modified and applied in more specialized fields.

SSE-CMM addresses the planning, development, and management of security and security architecture for an enterprise. The levels in security are basic, planned and verified, well defined and coordinated, measurable and quantitatively controlled, and constantly improving. Within these levels, sub-levels are identified. In general, SSE-CMM recommends determining the organization's performance level across a number of security engineering and process areas and then addressing individual problem areas to improve overall maturity.

SSE-CMM brings a good deal of discipline to management and process areas. Any large organization which has addressed basic areas of security but wishes to formalize the process and develop a more architectural and broader outlook, can benefit from the assessment and recommended activities. However the model does not, strictly speaking, advise on security activities and protections as such.

Strictly speaking, an organization need not necessarily aspire to the top or even the upper maturity levels: management has to determine what's appropriate for them in their particular situation at any given time. This gives management a degree of latitude that helps them align and prioritize work on security practices relative to other important strategic and commercial objectives.

### STIGs

No, this has nothing to do with the formerly anonymous professional racing driver on the BBC's Top Gear program. NIST, NSA and DISA/DoD have jointly developed several **Security Technical Implementation Guides (STIGs)** and related documents covering such security topics as Active Directory, application security, biometrics, database security, desktop applications, DNS, DSN (Defense Switched Network), enclave security, network infrastructure, Secure Remote Computing (SRC), Sharing Peripherals Across the Network (SPAN), UNIX & Linux & various flavors of Windows, VoIP, Web server and wireless networking. The STIGs would make excellent donors for corporate technical security standards and are highly recommended, along with the SP800 series.

### TickIT and ISO 9000

**TickIT** is a software **Quality Assurance (QA)** framework from the British Standards Institute built upon the foundations of **ISO 9000**. QA is extremely relevant to IT security: software and even

some hardware must meet confidentiality, integrity and availability requirements (for example being free of bugs, weaknesses or flaws that create security vulnerabilities) and deliver necessary security operations and audit functionality (such as event logging and analysis, and access rights management) in order to be 'fit for purpose'. The incessant patching treadmill clearly demonstrates that even allegedly well designed, painstakingly developed and thoroughly tested mass-market commercial software patently fails to meet perfectly reasonable quality objectives.

### Zachman Framework

The Zachman Framework is a two-dimensional model used to analyze an organization or process by breaking it down into smaller characteristics or considerations. Instead of trying to look at the entire enterprise at once, you break it down into a grid of perspectives and viewpoints. The "columns" of the framework are essentially an extension of the "five good serving men" *i.e.* "what" (entities or data), "how" (function), "where" (network), "who" (people or organization) "when" (time or schedule), and "why" (motivation). The rows of the model structure differing levels of scope and detail, generally following the phases of project management: overall scope and context (or ballpark view), business unit (system/process owner's view), system level (architect's view), technology level (designer's view), and the detail level (subcontractor or implementer's view).

The Zachman Framework is presented as a tool for analyzing architectural conditions and operations in business. However, the original intent was to address issues in regard to sharing data and the structuring of relationships in data warehouses. Therefore, while the tool would likely identify a number of important factors in regard to information flow, direct application to security will likely require some creative thinking on the part of the analyst.

For pictures of the Zachman Framework, see [www.zifa.com/framework.html](http://www.zifa.com/framework.html)

### Conclusion

While this awareness briefing can only give the merest introduction to the security frameworks themselves, we have provided a general idea of the types of frameworks that are available, plus the areas of relevance and application for specific frameworks. Hopefully you will also have noted that, just as no one security framework is suitable for all situations and applications, so no single framework should be relied upon as the sole guide for any enterprise. Multiple perspectives are necessary to provide a reasonable level of security and multiple frameworks have additional viewpoints to add to the construction of a well-rounded security architecture. Each folio (plus maybe others that we haven't even described) should ideally be considered to find out how it might enhance *your* security framework – that unique synthesis that belongs to your organization and supports your business strategies and information security policies.

### For more information

Visit the intranet Security Zone, contact the Information Security Manager or browse the [NoticeBored security compliance links](#) for more about compliance with security standards, laws, regulations *etc.* A companion technical briefing goes further into the pros and cons of compliance.

Please remember that this is only an awareness briefing, not legal advice. There are *many* other laws, regulations and standards than those mentioned and our interpretations are likely to be incomplete, wrong or misleading in specific circumstances and perhaps in general (we *are* only human!). As always for any topic concerning laws and regulations, **seek qualified legal advice**. Pay for a good lawyer or pay for a good lawyer.



### 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 contributions 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)