NOTICEBORED

Technical briefing

Information security rôles and responsibilities

Important note

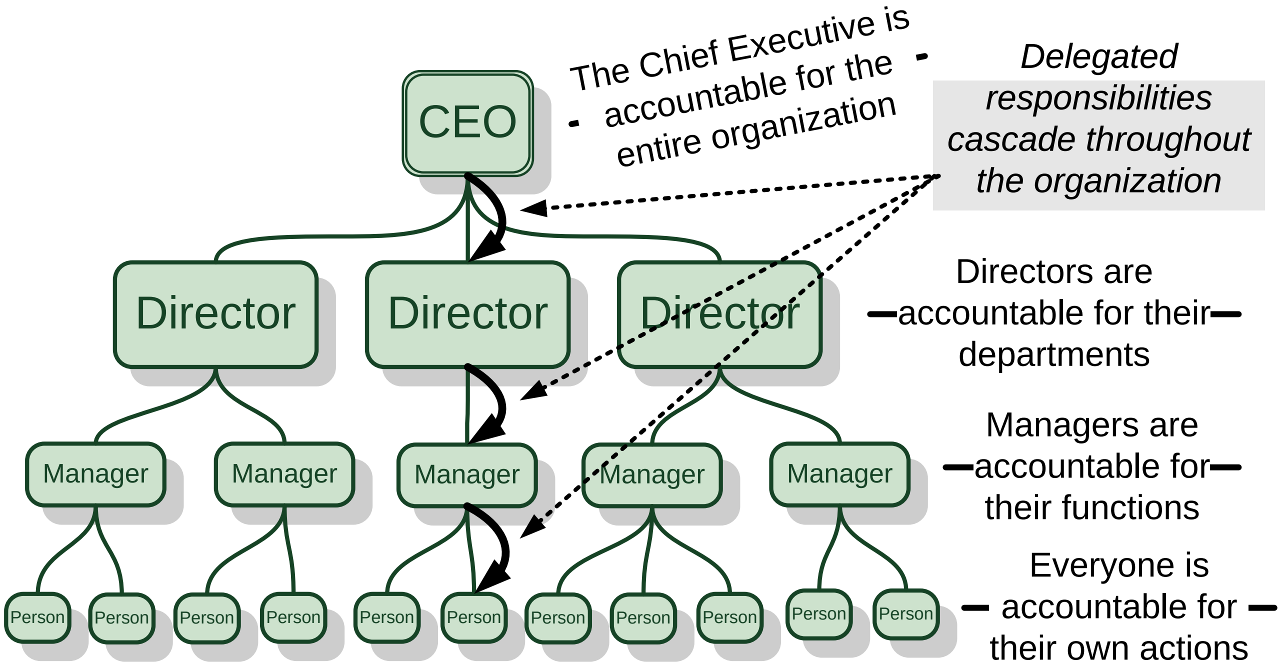
The requirements, rôles and responsibilities, and functions identified in this briefing are generic, do not necessarily apply to any given situation and may not suit your specific requirements. You should assess your own information security management requirements first and where possible reference existing rôles and responsibilities, departments *etc*.

Introduction

This briefing discusses the definition of information security management rôles and responsibilities based on the 39 control objectives identified in ISO/IEC 27002:2005.

General concepts

The dictionary defines accountability as “Being responsible or answerable to someone or for some action” while responsibility is “The state or position of having control or authority, or being accountable for ones actions and decisions; the ability or authority to act on one’s own, without supervision”. Responsibilities flow down through the organizational structure but normally ‘the buck stops’ at the top:


The Chief Executive is accountable for the entire organization
Delegated responsibilities cascade throughout the organization
CEO
Director
Director
Director
Directors are accountable for their departments
Manager
Manager
Manager
Manager
Manager
Managers are accountable for their functions
Person
Everyone is accountable for their own actions

Responsibility and accountability in relation to information security

Information plus the associated IT systems and networks are vital corporate assets widely dispersed throughout the organization. Therefore, according to the information security policy, information security is everyone's responsibility.

Information security responsibilities are defined in:

1. Policies, standards, procedures and guidelines mandated by senior management;
2. Contracts and agreements such as employment contracts and confidentiality agreements;
3. Applicable laws and regulations such as the data protection/privacy laws, Sarbanes-Oxley Act (SOX) *etc*.

The responsibilities are summed up by the definition of information security in ISO/IEC 27002, namely the protection of confidentiality, integrity and availability of information – and in a sense, we are all responsible for complying with ISO/IEC 27002 since it represents accepted good practice.

Trust and verification

Responsibility and accountability are supported by the concepts of trust and verification. Here are some simple examples to illustrate the point:

Information security trust example	Verification mechanism
Encryption protects credit card numbers when shopping on the web. Users trust that the encryption algorithms are strong enough to resist decryption and the implementations are flawless.	Third party certification programs such as WebTrust exist to verify that a website is, in fact, using appropriate encryption technologies correctly to protect online shoppers.
Users are trusted by management to choose strong passwords, not to share them and to keep other sensitive corporate or personal information secret.	System administrators, Information Security or IT Audit occasionally run password cracking programs against our own systems to identify weak password choices and castigate (*i.e.* call to account) the corresponding users.
System administrators are granted privileged access to IT systems on the understanding that they will not abuse their rights. They are trusted to behave responsibly. Professional qualifications are taken as evidence of their competence and experience.	Systems are configured to record use of privileges to secure audit logs, especially if there are highly sensitive/valuable data that are vulnerable to unauthorized access or modification by privileged users. System administrators, Information Security or IT Audit periodically check the audit logs, especially if there has been a system security incident.

The point is that, even though most things are taken on trust, compliance with information security responsibilities is monitored through a whole range of detective controls. This harks back to the paradoxical Cold War phrase "trust – but verify".

Information security incidents

If an information security incident occurs, the focus of attention normally moves through the organization structure in the opposite direction to responsibility, namely bottom-up. Say for example an end user is found to have caused a virus infection by opening an infected email attachment. He/she is likely to be firmly in the spotlight for his/her own actions or inactions, particularly if he/she did not follow antivirus policies and procedures, or if it appears he was negligent or deliberately opened the attachment. In addition, however, the broader situation that allowed such a mistake to happen may reflect badly on management (*e.g*. inadequate supervision, insufficient investment in antivirus controls), perhaps also technology management (*e.g*. improper configuration of the antivirus software, failure to identify that the antivirus software was ineffective). The CIO, Board of Directors or CEO might even be called to account if the virus infection led to severe impacts on the organization (such as extended system failures, disclosure of customer details or reputational damage). That example demonstrates the how the focus and scope of accountability varies at different levels within the corporate hierarchy.

Evidence

Imagine you are an independent manager investigating the virus incident noted above. Consider some of the questions arising from the situation described:

- How did the virus infection come to light? Did an antivirus scanner somewhere identify the problem? Was it was traced to an individual's PC using system access records? The network logon process with personal usernames and secret passwords unambiguously associates the user with his activities on the system, but can we be certain the user's passwords were not disclosed?
- Is it certain that the end user knew of his obligations under the corporate policies *etc*., in other words can it be proven that he had been explicitly informed of and understood his responsibilities? (Intranet records showing the user had visited the information security intranet pages and completed online antivirus awareness session would be ideal!);
- Could the user have denied responsibility or diverted attention to his manager, the systems administrators, the IT manager or someone else? If responsibilities were unclear, the chances of holding the user personally accountable for his actions are significantly reduced. Conversely, if those responsible for administering the antivirus system can prove the controls are effective, it seems likely that the virus was not detectable or that someone interfered with the antivirus controls, placing the focus back on the user.

Reliable evidence may be essential to get to the bottom of situations like this and assign accountability where it truly belongs. Remember that evidence can indicate innocence as well as guilt – if *you* were the antivirus system administrator in the example, would you be able to prove to someone that the system was working effectively? If not, your next pay slip might conceivably be your last.

Information asset ownership

The cascade of general responsibilities through the organization as shown above is reflected in the designation of information asset owners by management. Information Asset Owners are employees held accountable for protecting valuable databases, systems and other information assets on behalf of the organization. The Finance Director, for example, owns and has overall accountability for all the financial accounting systems, with ownership and accountability for individual systems typically being delegated to senior finance managers.

Information Asset Owners have the authority to determine what control measures are appropriate to protect their assets. They normally determine this by conducting a risk assessment and designing the controls in conjunction with risk and security control experts from Information Security, Risk Management *etc*. Implementation and operation of the controls is often dispersed amongst IT and other functions but the Information Asset Owners retain the right to review and modify the controls as they see fit. They have the ability, for instance, to decide what system access rules are appropriate, taking account of key control requirements such as division of responsibilities. Security Administration and IT Operations then apply the rules in practice.

Information security rôles and responsibilities matrix

Appended to this guideline is a generic matrix describing information security management rôles and responsibilities based on the 39 controls objectives in ISO/IEC 27002. There are columns for the people, functions or departments that are typically involved in managing information security although their titles and remits often differ between organizations. In the body of the matrix, we have made a start at identifying who is normally accountable for each control objective (*i.e*. where the buck stops), who is primarily responsible for designing and implementing the technical and procedural security controls to satisfy the objectives, other internal sources of consultancy/advice and those with "hands off" overview, review or governance responsibilities. Your mileage may vary.

Even if you are not using ISO/IEC 27002, the matrix to clarify rôles and responsibilities between business functions should still be useful for you.

Important procedural controls have to be properly defined by management and allocated unambiguously to the relevant individuals. This avoids situations where everybody assumes someone else is doing something, and nobody actually does it. The definition and allocation is conventionally achieved by:

- Analyzing business processes to determine risks and control points;
- Prioritizing the control points to identify key controls;
- Documenting the controls in procedures, job descriptions, training manuals *etc*.;
- Associating the procedures *etc*. with particular roles in the department;
- Allocating individuals to the rôles;
- Educating the individuals as to their obligations, especially the key controls;
- Monitoring the correct operation of the controls;
- Maintaining the procedures *etc*. to reflect changes and to ensure that controls are not compromised or forgotten.

Conclusion

We all share certain responsibilities for information security, a vital element of corporate governance, but we are individually accountable for our own actions. We are obliged to understand and fulfill our information security responsibilities or else risk being called to account.

For more information

For general advice on information security controls including those identified in this briefing, contact the Information Security Manager, visit Information Security's intranet website or browse the hyperlinks to useful accountability and related web resources on the NoticeBored links page. A generic procedure for defining information security rôles and responsibilities is available, along with policies and other awareness materials.

ISO/IEC 27002 itself is, of course, the main reference for this paper. Online resources include COBIT from ISACA and the Information Security Forum's Standard of Good Practice for Information Security. Useful books include the CISO Handbook by Gentile, Collette and August; the Handbook of Information Security Management by Krause and Tipton (or indeed almost any information security textbook); Writing Information Security Policies by Scott Barman; and Information security policies, procedures and standards - guidelines for effective information security management by Tom Peltier.

ISO/IEC 27002 section	Information security control	Department, function or rôle*							
		CEO	CIO	ISM	RM	HR	LRC	Sec	IAO
5.1	Information security policy plus management support & commitment	A	C	C	O	C	C	C	R
6.1	Management framework & rôles for information security management	A	C	C	O				R
6.2	Control third party access and products		A	R	O			R	O
7.1	Information asset owners identified and held accountable		R	C	O			R	A
7.2	Classify information assets		R	C	O			R	A
8.1	Pre-employment screening			C	O	A			R
8.2	During employment: awareness, training & education		C	R	O	A			R
8.3	Post-employment exit processes			C	O	A			R
9.1	Physical security for computer facilities		R	C	O			A	
9.2	Physical security for IT equipment, cabling *etc*. including safe disposal		R	C	O			A	R
10.1	IT operating procedures and responsibilities		A	R	O				
10.2	Manage third party service delivery		A	R	O		C		
10.3	Capacity planning and management		A	C	O				
10.4	Malware protection		A	R	O				
10.5	Backups		A	R	O				
10.6	Network security management		A	C	O				
10.7	Secure handling of storage media		A	C	O				
10.8	Formal agreements for data exchange with third parties		R	C	O		A		R
10.9	eCommerce security		A	R	O				O
10.10	Network and systems monitoring, logging and review		A	R	O				

* CEO = Chief Executive Officer. CIO = Chief Information Officer and IT Department generally. ISM = Information Security Management. RM = Risk Management. HR = Human Resources. LRC = Legal and Regulatory Compliance. Sec = Physical/site Security. IAO = Information Asset Owners or managers.

A = Accountable. R = Responsible. O = Oversight and review. C = Consultancy and advice.

ISO/IEC 27002 section	Information security control	Department, function or rôle*							
		CEO	CIO	ISM	RM	HR	LRC	Sec	IAO
11.1	Business requirements for access to information assets		R	C	O				A
11.2	Network/systems access rights for users		R	C	O				A
11.3	User responsibilities including access passwords and clear desks		R	C	O				A
11.4	Network access controls for users and automated interfaces		A	R	O				
11.5	Authenticating and logging systems access by users		A	R	O				
11.6	Access rights within application systems		R	C	O				A
11.7	Secure mobile computing and teleworking		R	C	O				A
12.1	Security/control requirements defined early in systems development		C	R	O				A
12.2	Data validation on inputs, processing and outputs		R	C	O				A
12.3	Cryptographic policy *e.g.* algorithms, key management		A	R	O				
12.4	Security for system files and test data		A	R	O				
12.5	Secure project and support environments, and control changes		R	C	O				A
12.6	Manage technical vulnerabilities in applications and operating systems		A	R	O				
13.1	Report events and weaknesses to a central point of contact		A	R	O			R	R
13.2	Manage security incidents, forensics and continuous improvement		R	A	O				
14.1	Manage business continuity and IT disaster recovery	A	R	C	O				R
15.1	Comply with laws relating to IT and information	A	R	R	O	R	R		O
15.2	Review systems & procedures for compliance to standards & policies		A	R	O	R	O	O	O
15.3	Control access to audit information and use of audit tools		A	R	O		O		O

*** End of list ***