A blueprint for an Enterprise Information Security Assurance System

Acuity Risk Management LLP

Introduction

The value of information as a business asset continues to grow and with it the need for effective information security. A wide-range of security products are available, and used, but we still appear increasingly vulnerable to security failures, both within our organisations and through the supply / customer chain.

Facing threats of regulatory censure, loss of customers or even prosecution if their information management falls below expected standards, Executives are increasingly looking for **assurance** that their information is being managed securely.

The popular ISO 27000 series of international standards for Information Security Management Systems (ISMS) were designed to provide assurance to senior management and other stakeholders that information security policies, processes and practices are based on an understanding of the risks to the business and are effective and sufficient for the needs of the business. Certification programmes have been developed world-wide to provide independent assurance that these management systems are (and continue to be) effective.

Although ISMS requirements and processes are relatively well-defined, the practical implementation of management systems, Enterprise-wide, is still in its infancy.

This paper describes a blueprint for **Enterprise Information Security Assurance Systems**.

Although this paper focuses on Enterprise Information Security Assurance Systems, the principles are applicable to any management system solution, including Quality Management Systems (ISO 9000 series), Environmental Management Systems (ISO 14000 series), Occupational Health & Safety Systems (ISO 18000 series) and Business Continuity Management Systems (BS 25999 series).

Governance vs Assurance

Before Executives can expect assurance, they need to set objectives, targets and strategy, i.e. they need to establish a system of **governance** against which assurance will be delivered. For information security, governance will involve:

- Setting information security strategy & direction
- Defining criteria by which information security risks will / will not be accepted
- Specifying performance indicators or targets, e.g. to keep risk within appetite, to maintain compliance levels above certain thresholds, to limit losses from incidents to a target level
- Defining requirements for assurance, e.g. the information security standards that the organisation will comply with, the types of risk that will be managed and whether there are variations in these requirements across the organisation.

Assurance is concerned with enabling the system of governance, i.e. through:

- Scoping the information security standards and the way that they will be applied across the organisation to meet the governance requirements
- Designing, and operating the assurance processes
- Identifying, assessing and measuring applicable risks, controls and events (incidents and near-misses)
- Informing governance, through effective and meaningful reporting.

The requirements for Information Security Assurance

The key first steps in implementing an assurance system are to determine the information security compliance requirements (e.g. ISO 27001, ISF Standard of Good Practice etc.), the risk types and to define the scope. For an ISMS, the scope is likely to include:

Information assets	Business processes
Teams	Third party organisations
Customers	Business application systems
Platforms	Critical services
Networks	Media
Sites / buildings	

Management will want various assurances in relation to the components within scope, referred to here under a broad definition as **'Assets'**. The most important assurances are as follows:

Assurance that:

- all material Assets within scope have been identified
- all Controls that are applicable to Assets within scope have been identified and all Controls are operating effectively within tolerances set by management
- all Risks to Assets within scope have been identified and all Risks are contained within management's appetite for risk.

Management will also want assurance that the management system reacts to change and is kept up to date. For example, if a new application system is brought within scope of an ISMS, management will want assurance that all risks relevant to that application have been identified, assessed and treated and continue to be managed within risk appetite. Management will also want assurance that all controls relevant to the application are operating effectively.

Within large organisations, management will want assurance that the above requirements are being delivered consistently Enterprise – wide.

Challenges in delivering Information Security Assurance

There are several information security assurance challenges that, in the past, have proved difficult to overcome.

1. **Up to date assurance status**. Organisational objectives and structures, their information handling requirements, threats and control performance change regularly and Executives can only receive assurance if the relevant information is accurate and current.

2. **Structure around business assets.** Risks and controls apply to business assets (information, applications, teams etc.) some of which are local, but others (such as corporate networks and enterprise applications) which may be shared. Risk and control compliance assessments are likely to vary between different assets and these variations must be visible to Executives seeking assurance.

3. **Granularity of analysis and reporting.** Management may want assurance in relation to assets, groups of assets, business units, business processes, regional views, Enterprise-wide views etc. It should be possible to report assurance status to Executives depending on their specific responsibilities and areas of interest.

4. **Assessment versus Measurement of control effectiveness**. The effectiveness of controls is a critical measurement for information security assurance. Without this, it is impossible to have confidence that controls are mitigating risk as anticipated. Simply confirming the existence of a control is not enough, nor is subjective assessment of performance. It is important to look for quantifiable performance indicators or metrics against which targets can be set and measured.

5. **Action tracking**. Actions which are identified to improve control effectiveness, address vulnerabilities, implement new controls, transfer risk etc. must be tracked through to completion. As actions are completed they will affect the current assurance status (in a positive way) and this should be visible to management (as per item 1).

6. **Integration with other systems**. Various other systems may provide data for the information security assurance system, e.g. metrics on the performance of certain controls, assets registers, document management systems / Intranet. Integration with these systems will usually be beneficial for more efficient assurance systems.

7. **Extension of assurance to third parties**. Most organisations are dependent on (or part of) a supply / customer chain with which they share information. Relationships with third parties, and respective information security obligations, may be governed by contracts or other agreements as defined by the system of governance. Executives will want assurance that their information is being managed securely by third parties.

8. **Setting and using risk thresholds and appetite**. In order to have assurance that information is being managed with an acceptable level of security, management needs to define thresholds for deciding which risks are acceptable / unacceptable and their appetite for information security risk, which may vary across the organisation. It must be possible to measure current risk status and compare with risk thresholds and appetite.

These challenges are all addressed in the blueprint described below.

Blueprint for an Enterprise Information Security Assurance system

The following blueprint is drawn from Acuity's experience in implementing information security assurance systems for major organisations across virtually every business sector. The blueprint is provided as a table with each row describing four factors: a requirement, features to deliver the requirement, benefits of the features and the impact if the features are missing. Requirements are grouped into the following sections:

1. Scope and asset management
2. Measurement of control effectiveness
3. Measurement of risk
4. Integration and change management
5. Aggregation, grouping and reporting
6. Ease of deployment and use
7. Performance, scalability and security

1. Scope and asset management

1	Scope and asset management			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
1a.	Assurance that all assets within scope will be identified	Specification of Asset Classes covering all categories of asset within scope. Checks that all assets from each Asset Class have been included in scope.	Management assurance that: o all assets have been identified o a consistent approach is being taken across the Enterprise	The absence of an asset-based approach will lead to an over-simplified system which cannot provide any meaningful assurance.
1b.	Assurance that all control requirements will be identified	Link control standards to Asset Classes so that, when an asset is brought into scope, the list of relevant controls applicable to that asset is created automatically	Management assurance that: o all relevant controls have been identified o a consistent approach is being taken across the Enterprise	
1c.	Assurance that all risks will be identified	Link threat lists to Asset Classes so that, when an asset is brought into scope, the list of relevant risks is created automatically	Management assurance that: o all relevant risks have been identified o a consistent approach is being taken across the Enterprise	
1d.	Assurance that key risk mitigating controls will be identified	Link key risk-mitigating controls to threats so that, when an asset is brought into scope, the list of key mitigating controls for each risk is created automatically	Management assurance that: o key risk mitigating controls have been identified o a consistent approach is being taken across the Enterprise	Inconsistent approach across different assets and weak assurance.
1e.	Handling of	Allow assets to be either local to	Avoids duplication of effort.	Less accurate and inefficient

1	Scope and asset management			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
	shared assets	management systems or shared between management systems. This allows risks to be assessed in relation to individual or groups of management systems and means that controls to shared assets only need to be assessed once.	Accurate modelling of the 'real world' situation where the business can be highly dependent on critical shared assets.	assurance processes prone to error through the need re-enter the same data multiple times.
1f.	Handling of dependencies between controls	Allow controls to be made dependent on multiple other controls so that a control (such as a business continuity plan) can only be considered effective if the controls on which it depends (such as data back-up, testing, maintenance etc.) are also effective.	Accurate modelling of the 'real world' situation where controls rarely act in isolation to each other.	Less accurate assurance reporting through inability to model the 'real world'.

2. Measurement of control effectiveness

2.	Measurement of control effectiveness			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
2a.	Assurance that controls are effective in	Assess the implementation of controls by taking into account a variety of factors which are	Management assurance that implemented controls are effective and mitigating risk as anticipated.	Most compliance products concentrate on assessing whether or not

2.	Measurement of control effectiveness			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
	operation	important for a mature and stable control, e.g. clear ownership, adequate documentation and evidence and fitness for purpose. Measure KPIs for controls to determine whether they are effective in operation and within tolerable thresholds.		controls/processes are in place, and ignore whether or not they are effective in operation. The existence of controls doesn't provide any assurance to management, it is their effectiveness at mitigating specific risks which is important.

3. Measurement of risk

3	Measurement of risk			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
3a.	Automatic calculation and recalculation of residual risk	In most risk management tools, residual risk is estimated by the user. This is highly subjective and gets out of date quickly as threats change or as the performance of key risk mitigating controls changes. Residual risk should be calculated automatically and recalculated every time a component of risk changes	More accurate risk assessments. Residual risk status always up to date with latest risk information. Easy to understand and use.	Laborious and inaccurate estimates of residual risk, leading to weak assurance.

3	Measurement of risk			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
3b.	Measurement of risk in relation to risk appetite	Set risk appetite in multiple ways to match business understanding and requirements. Calculate and report residual risk in relation to risk appetite.	Demonstrated compliance with 'best practice' risk management. Management visibility of risk status and whether or not action is required.	No criteria against which to decide whether or not risks can be accepted leading to weak assurance.

4. Integration and change management

4.	Integration and change management			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
4a.	Multiple management systems in a single assurance framework	Manage multiple, related control standards and risk types within a single assurance framework. Create an Integrated Management System for, say, ISO 27001, ISO 9001, ISO 14001, and ISO 18001 with each control standard and set of risks assessed using a suitable set of criteria.	Improved efficiency and effectiveness from avoiding silos and taking a consistent approach across all management systems.	Less efficient management systems, prone to inconsistency and error.
4b.	Integration of key management system	Integration of risk, compliance, metrics and incident management based around common asset models and linked control standards.	Management visibility of true compliance and risk status taking account of performance metrics for key controls and incident history.	Inability to understand true compliance and risk status leading to very weak assurance.

4.	Integration and change management			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
	components			
4c.	Adaptability to change	Automatic update of the risk and compliance framework whenever the management system scope changes (e.g. new functions, merged departments, new business applications, third parties etc.)	Accurate risk and compliance modelling of the Enterprise as it changes.	Inefficient assurance processes, risk of inaccurate assurance reporting.

5. Aggregation, grouping and reporting

5	Aggregation, grouping and reporting			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
5a.	Aggregation and grouping	Aggregation of views from local management systems to groups of management systems and Enterprise-wide. Provide multiple 'assurance' views for risk and compliance monitoring purposes, e.g. customer views, process views, organisation views, services provided.	Multiple management views for different layers of management and stakeholders, allowing earlier action to be taken to deal with unacceptable risks or major non-compliances.	Less efficient reporting on assurance.
5b.	Reporting	Real-time, on-demand graphical reporting via dashboards and on-	Highly visual easy to understand, 'at a glance' reporting for senior	Less effective communication of assurance status to

5	Aggregation, grouping and reporting			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
		screen reports. Export of data from to MS Excel workbooks for additional reporting and distribution.	management with detailed back-up reports for further analysis.	Executives.
5c.	History	Historical reports on risk, compliance and incident status.	Visibility of progress being made in lowering risk levels, improving compliance and reducing numbers and costs of incidents. Also, demonstrating the overall value of an ISMS	Inability to determine whether actions and associated expenditure are having the expected effect.

6. Ease of deployment and use

6	Ease of deployment and use			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
6a.	Assistance with complex and time consuming tasks	Business impact and threat likelihood assistants to create rapid risk assessments for review and approval by management.	Very quick and easy to use risk assessments which still produce rigorous risk data.	Less efficient assurance processes.
6b.	Configurability	Options to configure schemes for risk assessment, control assessment, metrics and event management.	Ability to support users' preferred risk and compliance processes rather than users having to adapt their methodology to accommodate a software solution.	Possible user-resistance to the assurance system

6	Ease of deployment and use			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
6c.	Importing from spreadsheets	Importation of any data held in spreadsheets including clients' own control standards, asset registers, previous compliance assessments or risk assessments.	Quick and easy to automate existing processes and to backload historical data.	Less efficient assurance processes.
6d.	Extended control assessment	Import of control assessment questionnaires and automatic collection of data from scanning and logging systems.	Efficiency improvements and maximising the return from existing processes and systems.	Less efficient assurance processes.

7. Performance, scalability and security

7	Performance, scalability and security			
No.	**Requirement?**	**Features to deliver the requirement?**	**Benefits of the features?**	**Impact if the features are missing?**
7a.	Performance and scalability	Scalable and high-performance system with ability to add management systems, risk registers, assets, threats, controls and incidents without degradation of performance	Fast, responsive user experience with risk and compliance status automatically calculated and reported in real-time.	Possible user – rejection of the assurance system. No future – proofing.
7b.	User management and security	Users are given read-only or read-write access to only those dashboards, screens and reports that they have been authorised to access.	Management confidence that sensitive information is only accessible to authorised users.	User rejection if an information security assurance system can't provide adequate security.

Summary

Executives will increasingly demand assurance that information is being managed securely (both internally and throughout the supply / customer chain) in accordance with their defined system of governance.

Sophisticated software solutions are available today that can deliver the blueprint outlined in this paper and provide substantial efficiency and effectiveness benefits. Most importantly, management and stakeholders can gain assurance that information security is being managed and maintained in accordance with their wishes.

Further information

For further information, please contact Simon Marvell or Richard Mayall.

Simon Marvell is a Partner and Managing Director of Acuity Risk Management LLP. He has over 25 years experience implementing risk management processes and solutions across almost every business sector. Prior to founding Acuity, Simon was a founding Partner and Managing Director of Insight Consulting, a UK based professional services firm which he sold to Siemens plc in 2004.

simon.marvell@acuityrm.com

Richard Mayall is a Partner and Director of Technology & Applications at Acuity Risk Management LLP. He has over 25 years experience in information security management systems and assurance and is a visiting lecturer on these subjects at University of London, Royal Holloway College. Prior to founding Acuity, Richard led the information security consultancy practice at Insight Consulting.

richard.mayall@acuityrm.com

Acuity Risk Management LLP
Liberty House
222 Regent Street
London W1B 5TR

+44 (0) 20 7297 2086
www.acuityrm.com