

Security Domain Roadmap

Technology Roadmaps

DOCUMENT CONTROL

Document Details

Document Owner	Tony Bright
Document Author	Mark Cooper
Current Version	1.1
Issue Date	
Programme Reference	Enterprise Architecture
Project Reference	Enterprise Architecture Security Domain

Revision History

DATE	VERSION	CHANGE DETAILS
24 th April 2008	1.0	Initial Version
30 th April 2008	1.1	Updated after initial review

Distribution

DATE	VERSION	DISTRIBUTION
24 th April 2008	1.0	Tony Bright, Kapila Munaweera, Phil Burnham and Terry Pyle for initial review
30 th April 2008	1.1	Architecture Program Board

TABLE OF CONTENTS

1.0	Introduction.....	4
1.1	Objectives.....	4
2.0	Executive Summary	5
2.1	Relationship to outsourcing	6
3.0	Security Domain Architecture Description.....	6
3.1	Position of the Security Domain within the overall British Council Enterprise Architecture.....	9
3.2	Future Capability Summary	9
4.0	Direction of Travel	11
4.1	Business changes impacting the Security Domain.....	11
4.2	Architectural and technical opportunities.....	12
4.3	Overview of Change	13
4.4	Future Capabilities.....	14
4.4.1	Risk assessment framework.....	15
4.4.2	Security architecture governance	15
4.4.3	Global security operations and monitoring capability	15
4.4.4	Incident management program.....	15
5.0	Detailed Description	19
5.1	Logical Domain Model(S)	19
5.1.1	Security Architecture Life Cycle.....	19
5.2	Physical Domain Model(s).....	20
5.3	Enterprise Security Domain Roadmap	21
6.0	Making it Happen	24
6.1	Technology Choices	24
6.1.1	Security Incident Cost Calculator.....	24
6.1.2	Risk Assessment Matrix	25
6.1.3	Crisis Management Manual	26
6.1.4	Incident Management Handbook.....	26
6.2	Key Organisation Processes	26
6.3	Resources and Skills, Provision Assumptions.....	26
6.4	Milestones and Deadlines	28
6.5	Domain Strategic Roadmap	30
6.5.1	Step 1 - Establish Risk Assessment Framework	30
6.5.2	Step 2 - Establish Security Architecture Governance.....	30
6.5.3	Step 3 - Set up Global Security Operations & Monitoring.....	30
6.5.4	Step 4 - Introduce Security Incident Management.....	30
7.0	Appendix 1 - Principles Guiding the Security Domain.....	31
7.1	Business Principles	31
7.2	Functional Principles	31
7.3	Technical Principles.....	31

7.4	Governance Principles	31
8.0	Appendix 2 - References.....	32

TABLE OF FIGURES

Figure 1 - British Council Enterprise Architecture	9
Figure 2 - Information Security Life Cycle Architecture.....	10
Figure 3 - Security jigsaw - Policy, People and Products.....	12
Figure 4 - Enterprise Architecture Security Domain Benefits Matrix.....	14
Figure 5 - Incident Management Program Areas.....	16
Figure 6 - Information Security Life Cycle Architecture.....	19
Figure 7 - Operational Security Management Information Flow.....	20
Figure 8 - Security Management Technical Architecture	21
Figure 9 - Security maturity	21
Figure 10 - Security maturity scorecard	23
Figure 11 - Security Incident Cost Calculator.....	24
Figure 12 - Calculating downtime costs	25
Figure 13 - Typical Security Organisation Structure	28
Figure 14 - Security Domain Strategic Roadmap.....	30

TABLE OF TABLES

Table 1 - Security Domain Strategic Approaches	5
--	---

1.0 Introduction

This document describes the target architecture roadmap for the Security Domain.

1.1 Objectives

The objectives of this document are:

- To provide a summary of the roadmap for the Security Domain
- To communicate an understanding of the Security Domain target architecture to stakeholders at an appropriate level of detail
- To position the Security Domain within the overall British Council enterprise architecture and describe the capabilities covered by this domain
- To describe how the business direction and technology opportunities have shaped the target domain architecture
- To explore the options available to the British Council for this domain
- To identify the major deadlines and milestones for the delivery of the capabilities provided by this domain
- To identify at a high level the resources and skills required to implement the capabilities
- To describe the Security Domain roadmap

2.0 Executive Summary

The key question that the British Council needs to address is ‘how much security is enough’. There needs to be balance established between cost and risk, and as with the other enterprise architecture domains, the requirements for security must come from the business.

There are many ways for any business to go offline: human error, power outages, security & service attacks, and of course natural and man made disasters. It is not just the IT infrastructure; the entire continuum of service availability must be addressed.

The real cost of the Council going ‘off-line’ or experiencing a leak of sensitive information needs to be assessed. This can then be used to drive an effective security program within IT. Generally, organisations tend to underestimate the business and reputation risks of service availability failures (whatever the cause).

In some security scenarios, for example, a significant proportion of the British Council could go offline – effectively and closing all operations to employees and customers. Service continuity is therefore not just about disaster planning (one off events/contingencies) but about implementing a rigorous approach to service availability planning.

The current approach adopted by the Council tends to be ‘bottom-up’¹, and while this is pragmatic may not necessarily meet the current or future needs of the business.

Establishing an enterprise-wide *risk assessment framework* is the first step to understanding the IT security requirements. Urgent steps should also be taken to roll out infrastructure patches where these have yet to be applied.

Priority	Initiative	When	Key Benefits
Very High	Roll out infrastructure patches	ASAP	<ul style="list-style-type: none"> Reduced operational risk
Very High	Establish risk assessment framework	ASAP	<ul style="list-style-type: none"> Reduced operational risk Optimise IT cost
High	Security architecture governance	By end 2008	<ul style="list-style-type: none"> Reduce operational risk Reduce procurements cost² Reduce support cost³
High	Global security operations and monitoring	By mid 2009	<ul style="list-style-type: none"> Reduced operational risk
Medium	Security incident management	By mid 2010	<ul style="list-style-type: none"> Reduced operational risk Reduced support cost (over time)

Table 1 - Security Domain Strategic Approaches

Once the risk assessment framework has been established, a much deeper understanding of IT security requirements will emerge. However, based on experience with other customers, and an initial high-level understanding of the needs of the Council, it is likely that putting in place *Global*

¹ E.g. antivirus

² It is more cost effective to factor in security early in the solution development/procurement lifecycle

³ Reduce the need to implement security measure post implementation

security operations and monitoring and *Security incident management* will be appropriate measures. These are both functions of service management.

Global security operations and monitoring ensures that the security state of the British Council is known at all times. The result will feed into security incident management who proactively and reactively address security issues.

To complete the security picture, strong security architecture governance needs to be put in place as soon as possible to ensure that all new solutions are compliant with the Council's security requirements. The Council's own risk assessments (which have not been produced) should thoroughly be reviewed in that process.

2.1 Relationship to outsourcing

The overall control of security is not something that the Council should consider handing over to a third party. However all suppliers of products and services to the British Council must be aware of, and compliant with the security requirements.

3.0 Security Domain Architecture Description

According to British Council's Business Risk Management Framework ^[Ref 1] the aim of the Security Domain is to ensure that:

“the confidentiality, integrity and availability of corporate information systems are maintained at all times through the development, monitoring and enforcement of a corporate information security policy that ensures that:

- *all systems are available to authorised users whenever they are needed and that adequate contingency procedures are in place to maintain availability in the event of a disaster;*
- *only approved software is operated and that appropriate and valid licences are held for all software operated;*
- *the procurement and development and disposal of IT equipment and software is managed in line with corporate information security policy;*
- *adequate and appropriate access rights are maintained and secure storage arrangements exist for information held to ensure that information may only be viewed by those with the appropriate rights to do so;*
- *the integrity of all data is maintained so that documents can be assured for completeness and accuracy at all times;*
- *All information is held and maintained in accordance with prevailing UK and European laws.”*

Roles and responsibilities

Although Information Security within the British Council is, to varying degrees, the responsibility of all members of staff, certain individuals have key roles defined in the Council's Information Security Policy:

- The Executive Board holds overall responsibility. This is significant, as failure to comply with legal or regulatory controls could lead to legal proceedings being brought against individual Board members.
- The Chief Information Officer (Global IS) has “direct responsibility for the security of the British Council's IT infrastructure and for the recommendation to the Senior Management Team of practices to be adopted throughout the organisation. He or she also has the responsibility for the coordination of information security initiatives.” One of the CIO's key security responsibilities is to appoint a Worldwide Security Manager.
- The Worldwide Security Manager is the Council member of staff who is an information security professional.
- Other specialist roles mandated by the ISP include a Data Protection Officer, Records Officer and Freedom of Information Officer.

Risk-based security strategy

In any organisation, risk management is a key driver to ensuring that an appropriate “quantity” of security is enacted and that typically limited resources are prioritised accordingly.

The Council has a risk analysis process, known as the Business Risk Management Framework ^[Ref 8]. This process is owned by the Head of Audit, and it appears to be focussed predominantly on financial controls.

Attempts to obtain current risk assessments of the Council's assets were unsuccessful, despite approaches to a number of sources. These should be immediately available to demonstrate that:

- the Council has security measures that are commensurate with the risks; and
- all risks have been identified and dealt with appropriately (transfer, avoid, reduce or accept)

Urgent follow up work is recommended.

Information Security Policy

The normal progression following on from a security risk assessment is the production of the security strategy and information security policy. The WSM has produced the Information Security Policy (ISP) ^[Ref 2]. The Information Security Policy is aligned to the industry best practice ISO27001 standard, and was recently updated and endorsed by senior management. It is “*recognised as being vital in supporting the British Council's activities and our 2010 strategy*”. ^[Ref 2]

IT Security

The Council's IT infrastructure, and thus its digital information, is highly distributed ^[Ref 3]. UK-based systems are primarily managed by LogicaCMG. The security provisions of their contract are set out in Schedule 2 of the applicable UK contract ^[Ref 5].

Support for overseas systems and data remains the responsibility of the Council itself, and thus so does the security of these systems and their data. Provision of the global network has been outsourced to a third party, Global Crossing, and their security responsibilities are documented in Schedule 1 of their contract ^[Ref 6].

Although mandated in their respective schedules, and despite direct requests, neither Logica nor Global Crossing is providing the WSM with the required security reports. The Council therefore cannot be certain that the controls that they have outsourced are appropriate or effective. More

alarming still, in the case of the global network provider the Council's Worldwide Security Manager was not consulted on the security elements of the contract!

Compliance

Security audits are required to ensure that the implementation and operation of security controls remain effective. Audits are conducted within the Council by a variety of groups at various intervals:

- The Council conducts IT audits using their own Audit team, with the security aspects being audited on their behalf by Deloitte & Touche. The last security audit was completed by Deloitte & Touche in December 2006, with the report being published in early 2007. It was a follow-up to their network audit conducted in 2003.
- The National Audit office conducts periodic audits.
- The WSM conducts regular reviews of Internet browsing logs, scans for unlicensed software and inappropriate content such as MP3 music files on servers.

“Business as usual” (BAU) security

Applying patches in a timely manner is an unfortunate but regular necessity with modern IT systems. The Council has Change and Release Management processes and infrastructure ^[Ref 4]. However, it is noted that the Council is **at least** 6 months behind Microsoft's release cycle for critical infrastructure and security patches.

3.1 Position of the Security Domain within the overall British Council Enterprise Architecture

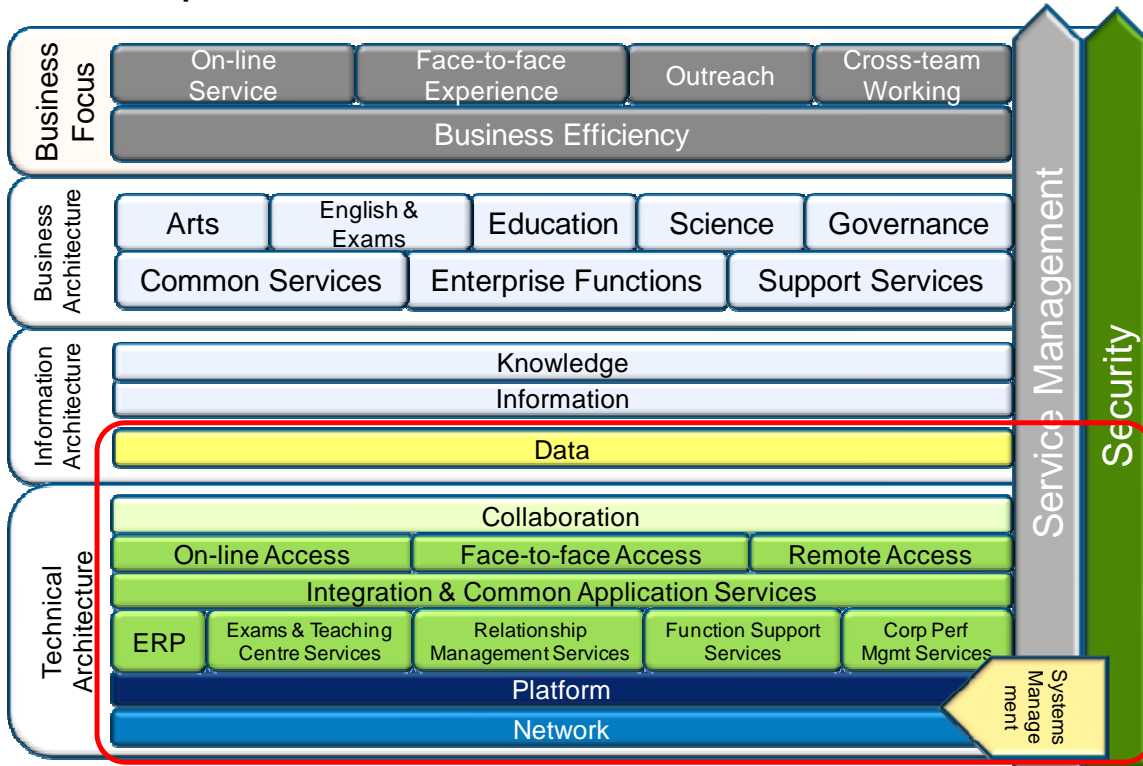


Figure 1 - British Council Enterprise Architecture

3.2 Future Capability Summary

The Security Domain, like the Systems Management Domain, cuts across all other domains within the Enterprise Architecture. There is a close relationship between the Security and the Systems Management domains, as both are concerned with governing and managing IT systems, data and components across the British Council infrastructure. Both of these domains are dependent on the implementation and operation of appropriate processes in order to ensure that their objectives are achieved. Moreover, both have the **same** objective, namely to help ensure the ongoing operation of the Council's IT-based services. Thus, the processes within these two domains should be integrated with each other to enable efficient and effective operation.

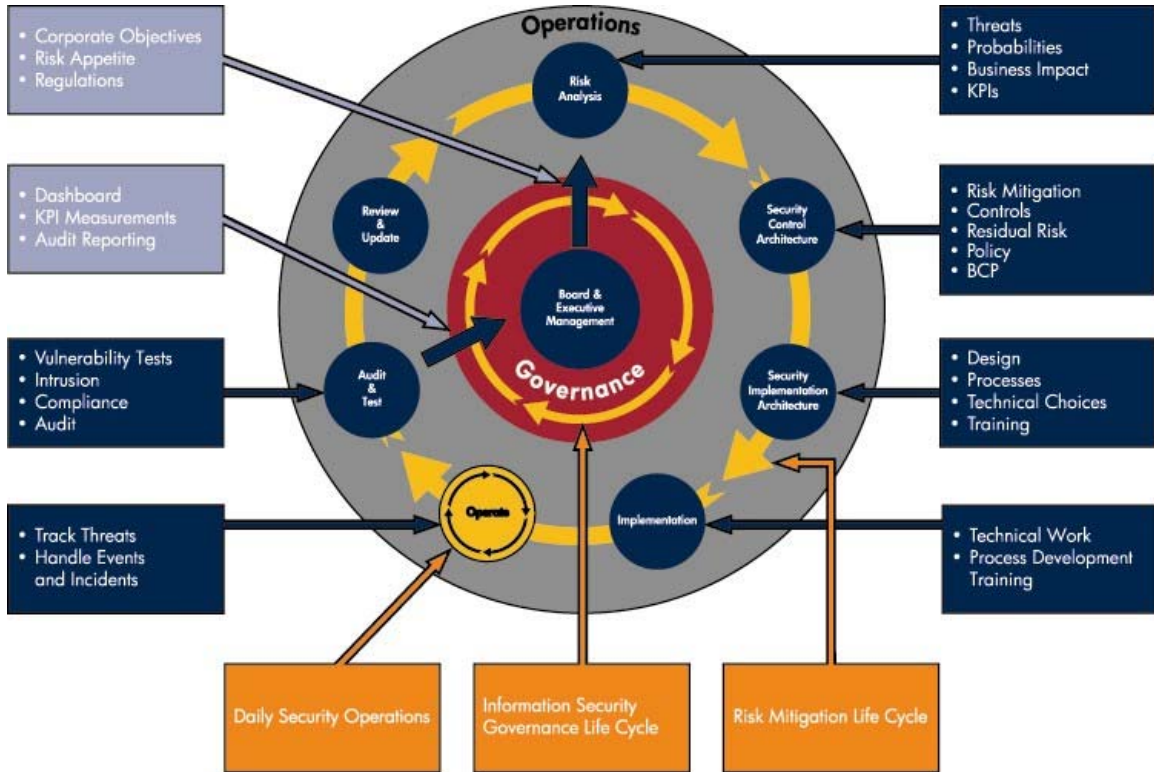


Figure 2 - Information Security Life Cycle Architecture

4.0 Direction of Travel

4.1 Business changes impacting the Security Domain

The British Council's business-driven enterprise architecture strategy^[Ref 7] includes a number of Principles that drive the Security Domain. These are:

- Business Principle 1 - Information as an Asset
- Business Principle 2 - Security Strategy
- Functional Principle 1 - Legal and Regulatory Requirements
- Functional Principle 2 - Confidentiality, Integrity and Availability of Data and Systems
- Functional Principle 3 - Security Policy
- Functional Principle 4 - Information Quality
- Functional Principle 5 - Business Continuity
- Technical Principle 1 - Industry Standards
- Technical Principle 2 - Security Standards
- Technical Principle 3 - Solution Characteristics
- Governance Principle 1 - Enterprise architecture is business driven
- Governance Principle 2 - Architectural values are to be publicised
- Governance Principle 3 - Architecture efforts must be unified across the Enterprise

Looking outside of the Council, recent national events have raised the public's awareness of security. Accounts of the bulk loss of individual's personal details, through theft of unprotected laptops or loss in transit of unprotected data disks seem to appear almost daily. The organisations at fault suffer damage to their reputation and brand image, and are at risk of fines and legal action, for instance under the terms of the Data Protection Act or FSA regulations. On an international scale, it is noted that the Council operates in territories that are not always friendly to the UK. There is a real risk that Council premises could be searched and systems and their data confiscated. In some territories, it is common for all foreign interests to be "bugged", with voice and data communications being intercepted and monitored.

For these reasons the Council must risk assess the impact to itself should such actions occur, paying particular attention to the potential damage to its reputation and consequent loss of business.

It is noted that the Council is leveraging recent Government focus on lost data to ensure that its laptops are provided with encryption. However, it is felt that the Council might be putting too much emphasis on short-term low software costs when choosing its solution, rather than looking at the long-term needs, operation complexities and total cost of ownership.⁴

It should also be noted that laptops are not the only potential source of lost data, and that the whole spectrum of storage devices, from physically small removable media such as USB keys, through portable devices such as PDAs to large office-based systems, must be considered. Additionally, the security of data in transit, whether inside an office, between local offices or globally across the WAN should be assessed.

⁴ home-grown Microsoft-based PKI solution providing keys for encrypted file systems

4.2 Architectural and technical opportunities

Pending the development of risk-based enterprise security architecture the Council must continue to rely on fundamental security best practises. Some, such as anti-virus, are already deployed. One way to establish a benchmark for the Council's baseline security state is through use of the Centre for Internet Security's security scoring tools ^[Ref 9]. This provides an industry-accepted assessment against minimum security standards for all common computing and network platforms, together with details on how to implement these baseline controls.

Others controls that should be considered include:

To promote confidentiality:

- Ensure that sensitive data is held securely. Enable application-level encryption of data
- Ensure that sensitive data is transmitted securely. Specifically this should focus on administrative user passwords. Enable IPSEC between offices and across the WAN. Enable IPSEC inside offices and/or a solution such as Apani to protect local traffic according to policies.

To promote integrity:

- Use a file system integrity⁵ checking mechanisms such as Tripwire or Symantec ESM. The highly standardised manner in which Council systems are built and patches are rolled out simplifies the deployment and maintenance of such tools. Furthermore, the use of integrity-checking tools provides additional benefits beyond pure security, in terms of configuration and change management.

Remember that security is not just product. People and Process are equally important.

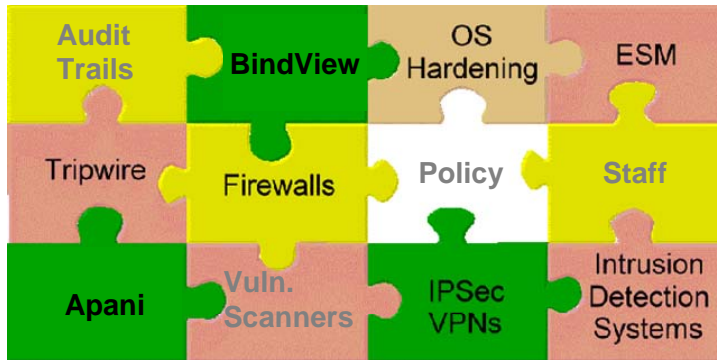


Figure 3 - Security jigsaw - Policy, People and Products

The Council must leverage the monitoring capabilities provided by its third parties to ensure that it is constantly aware of the threat levels.

The Council must drastically reduce its backlog of patches, currently reported at being in excess of 6 months. Given the uniformity of the Council's systems, any vulnerability will be replicated across hundreds of servers and thousands of PC in the absence of web security filtering system. The threat is not only that the Council is highly exposed to damage to its systems and data, with

⁵ especially valuable if used on the web servers hosted for external access

subsequent loss of business. There is also a highly credible threat that compromised and geographically distributed systems could be leveraged in an attack on an external third party. The weakening of the Council's outbound network filtering by Global Crossing only exacerbates this risk.

4.3 Overview of Change

As part of the Enterprise Architecture Roadmap exercise, a number of changes to the British Council's infrastructure and business practises are being proposed. Many of these changes will improve the overall security of the Council, further demonstrating that security is not a stand-alone discipline.

For instance:

- The various changes outlined in the Platform Domain document all result in a simplified and reduced overseas infrastructure. Having fewer systems to manage clearly results in less scope for operator errors, fewer potentially vulnerable devices as well as reducing the number of potential targets for attack.
- Improvements in systems management and monitoring will yield security benefits in terms of change management, release management and, most importantly, patch management.

		Security				
		Implement Short-term Security Fixes (e.g. Patches)	Risk Assessment Framework	Security Architecture Governance	Global Security Ops & Monitoring	Security Incident Management
Prioritisation Rating		34	29	28	14	12
Difficulty (1 = easy, 5 = difficult)		1	2	2	3	4
Cost (1 = low, 5 = high)		1	1	1	3	3
Dependency Factor (1 = has dependents, 5 = no dependents)		1	1	1	2	2
Benefit	Importance (1 = low, 5 = high)					
Increase business efficiency	5	1	3	2	2	2
Reduce operational risk	3	5	5	5	5	5
Faster time-to-market	3	1	1	1	1	1
Flexible business relocation	3	1	1	1	1	1
Flexible delivery channel support	2	1	1	1	1	1
Flexible working (e.g. 3rd parties)	2	1	1	1	1	1
Better access to information	4	1	1	1	1	1
Improve service quality	3	5	5	5	5	5
Improve scalability	3	2	3	3	3	2
Reduce IT costs	5	5	5	5	5	5
Strengthen compliance & security	4	5	5	5	5	5
Reduce training needs	1	1	2	2	2	2
Value (Higher = more value)		101	115	110	110	107

Figure 4 - Enterprise Architecture Security Domain Benefits Matrix

4.4 Future Capabilities

The key enterprise-wide security capabilities that the Council should be aiming to implement are described in the following sections.

4.4.1 Risk assessment framework

The risk assessment framework is needed to ensure that efforts and resources are prioritised appropriately and that all issues are addressed.

The aim is to identify, and value, the enterprise's assets, from the macro (enterprise-wide and business unit level) to the micro level (individual business or IT services). Risk analysis aims to identify vulnerabilities in the existing environments, threats that might exploit these vulnerabilities, and the impact ("cost") on the business should such a threat be executed. It is vital, as without it an enterprise cannot know what assets need protecting, or "how much" protection should be assigned to each asset.

The Council already has the Business Risk Management Framework (BRMF). However, although Information Security is included within the BRMF, it *appears* to be primarily focussed on ensuring financial accounting accuracy and legitimacy. The Council must ensure that detailed security-based risk assessments are also conducted, so that appropriate security architecture can be formulated.

4.4.2 Security architecture governance

It is easily demonstrated that the cost of attempting to "bolt on" security at the end stage of a project is far higher, and the result far less secure, compared to properly considering appropriate security during the design stages.

Security architecture technical capability is required to ensure that security is designed in from the outset for future business IS solutions. It should be made available to current and future projects. Where risk assessments indicate, it should be used to provide remedial security to legacy business services. As with other architectural elements, retaining these skills internally as opposed to outsourcing or contracting them in would help to ensure that the Council maintains a consistent view of security across the enterprise. It would also provide the Council with greater flexibility as its internal organisations and business units continue to evolve.

4.4.3 Global security operations and monitoring capability

A global security operations and monitoring capability is required to ensure that the security state of the Council is known. This should be a feed into the Service Management capability, on a par with Systems Management. It may also be required as a means of demonstrating regulatory and legal compliance.

4.4.4 Incident management program

An Incident Management Program is a coordinated program of people, processes, tools and technology, which prevents and manages information security threats, vulnerabilities and incidents in order to minimise their impact on a company or organisation.

It is needed:

- To ensure that security incidents can be contained controlled, cleaned up and lessons learned.
- To protect the Council's brand and reputation
- To protect the Council's intellectual property
- To ensure the Council's uninterrupted ability to conduct business

- To avoid lost customers and revenue
- To avoid the cost of lost productivity
- To avoid the cost of cleaning up the effects of security incidents on the IT infrastructure

“Young” incident management frameworks are typically focussed on reactive capabilities. The more effective (“mature”) frameworks understand that the key to success is to focus on the up-front planning. They recognise that there is no time during an incident to be formulating plans; value-based decisions will already have been made.

Incident Management covers a number of capabilities. Whilst reading the following descriptions please note that this document is not proposing that the Council implements all of the following functions and capabilities itself!

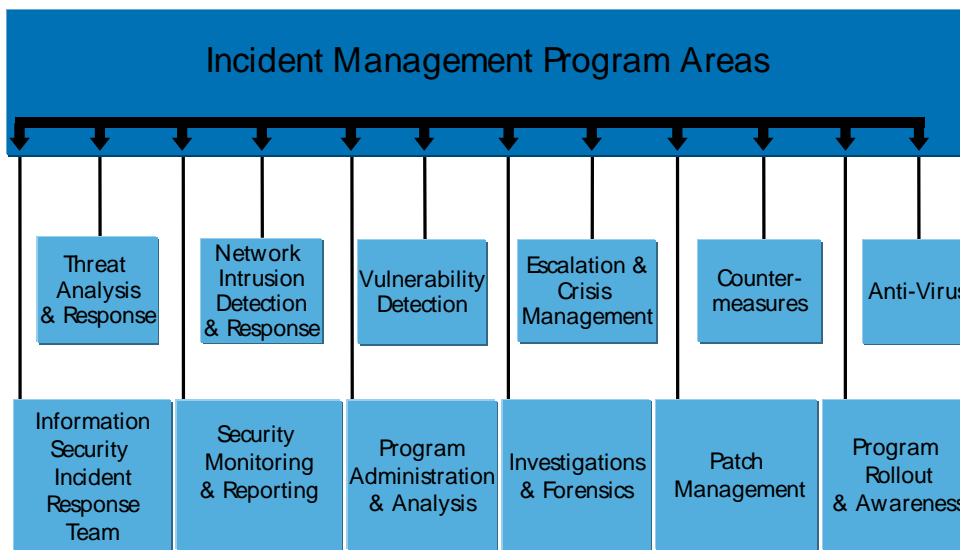


Figure 5 - Incident Management Program Areas

The Threat Analysis and Response Team:

- Proactively researches and monitors security-related information to identify information security threats that may impact your organisation
- Threats are analysed for their impact on the Council and assigned a risk classification
- Informational alerts and remediation requirements are developed and distributed to the appropriate parties throughout the Council
- This process ensures that threats are consistently addressed in a timely manner throughout the enterprise

The Network Intrusion Detection and Response Team:

- Proactively monitors the Internet-facing infrastructure for signs of network intrusions and other anomalous activities, traffic, etc. This involves ensuring that network intrusion detection sensor (IDS) alerts are properly addressed.
- Assists the Information Security Incident Response Team (ISIRT) in addressing detected attacks in real time
- Works in close cooperation with the Infrastructure Network Team related to the deployment and tuning of network-based intrusion detection sensors

Note that network intrusion detection is allegedly provided by Global Crossing and, in the UK, Logica CMG. However, **details** of such capabilities are not readily apparent in their respective contract schedules. In particular, what do the sensors classify as suspicious or hostile traffic? Without close liaison with the Council, any third party can at best use IDS sensors in their “out of the box” state, which will provide an extremely poor level of coverage, risking both highly dangerous false negatives as well as desensitising false positives.

The Vulnerability Detection Team:

- Conducts regular ongoing vulnerability scans/probes of the Internet-facing infrastructure to identify key high-risk vulnerabilities
- Provides vulnerability data to the Information Security Incident Response Team (ISIRT) so that the vulnerabilities are addressed
- Conducts “special request” scans of the infrastructure
- Rescans vulnerable systems to assess remediation status
- Assists in the management of exception requests related to vulnerability remediation

The Information Security Escalation & Crisis Management Team:

- Prepares for and addresses those unique information security-related incidents that are anticipated to cause significant impact or have caused enterprise-wide severe impact or interruption.

The vital phrase here is “prepares for”. Responses must have been decided in advance and plans prepared. Whilst at first sight this might seem impossible (“*We can’t know everything that is going to happen to the Council*”), it is perfectly feasible if considered at the correct level.

For instance, if one of the deployed security mechanisms detected that the SAP system was being attacked from outside of the Council, via the main Council website, what would be the most appropriate action? Options might include:

1. disconnecting the main Internet feed
2. switching off the main website,
3. disconnecting the SAP system
4. switching off the SAP system

On the basis that irreparable damage might be being conducted to the SAP databases, trying to identify, contact and liaise with all the appropriate Council and external authorities to make a rational decision is not something that should or can be done during the incident crisis. Consideration must be given to vacation, sick leave, lunch break, weekend etc.

The solution is to have populated the **Crisis Management Manual** with the appropriate scenarios and risk-based decisions, derived at having used the **Security Incident Cost Calculator** to analyse the results of the **Risk Assessment Matrix**. These tools are described in more detail later on.

The Information Security Anti-Virus Team:

- Plans and implements the Council’s Antivirus strategy (e.g., choice of tools, tool deployment, etc.)
- Obtains and tests new versions of Antivirus tools when they are made available

- Facilitates the communication of Antivirus strategy, directions and tools available

The Information Security Incident Response Team (ISIRT):

- Is a global team with corporate-wide responsibilities pertaining to receiving, assessing, responding to, addressing and managing information security incidents
- Depending on the severity of incidents, ISIRT will own, hand-off, address, or escalate security incidents, thus ensuring incidents are handled commensurate with their level of risk

The Information Security Monitoring and Reporting Team:

- Monitors patching compliance related to high-risk vulnerabilities for internal systems where these conditions can be remotely detected
- Works closely with regional and business security teams, IT delivery teams, and other teams within Information Security and the Information Security Incident Management Program.

The Program Administration and Analysis Team:

- Collects, consolidates, analyses and provides specific audience-based reports related to the functional programs within the Information Security Threat, Vulnerability and Incident Management Program
- This Team also conducts strategic planning and budgeting and leads the program/project management and maintenance activities within the Program.

The Information Security Investigations & Forensics Team:

- Addresses serious information security related incidents which involve civil, criminal, administrative, disciplinary, brand and/or financial implications
- Works closely with internal partners such as Legal, HR/ER, Media Relations and Security and external parties such as law enforcement and government authorities
- Has ability to recover, decrypt, and analyse IT-related data and report, present, and represent such data in civil, criminal, and administrative proceedings

The Information Security Patch Management Team:

- Works in conjunction with Threat Analysis and Response and Vulnerability Detection program areas
- Provides system owners with remediation information related to high-risk vulnerabilities affecting the company's infrastructure
- Creates weekly reports that track number of vulnerable systems detected and number of systems remediated

The Information Security Program Rollout and Awareness Team:

- Develops and delivers end-user and partner-focused communications and awareness activities to increase understanding, use of, and compliance related to the Information Security Threat, Vulnerability and Incident Management Program.

Section 6.3 below expands on the organisational structure that might be required to fulfil these roles.

5.0 Detailed Description

5.1 Logical Domain Model(S)

The diagrams below are to demonstrate that security is not just a collection of technological point solutions. It is a spectrum of controls, the requirements and specifications of which can only be determined once the assets have been identified and valued, the threats, vulnerabilities and consequential impacts qualified and quantified.

5.1.1 Security Architecture Life Cycle

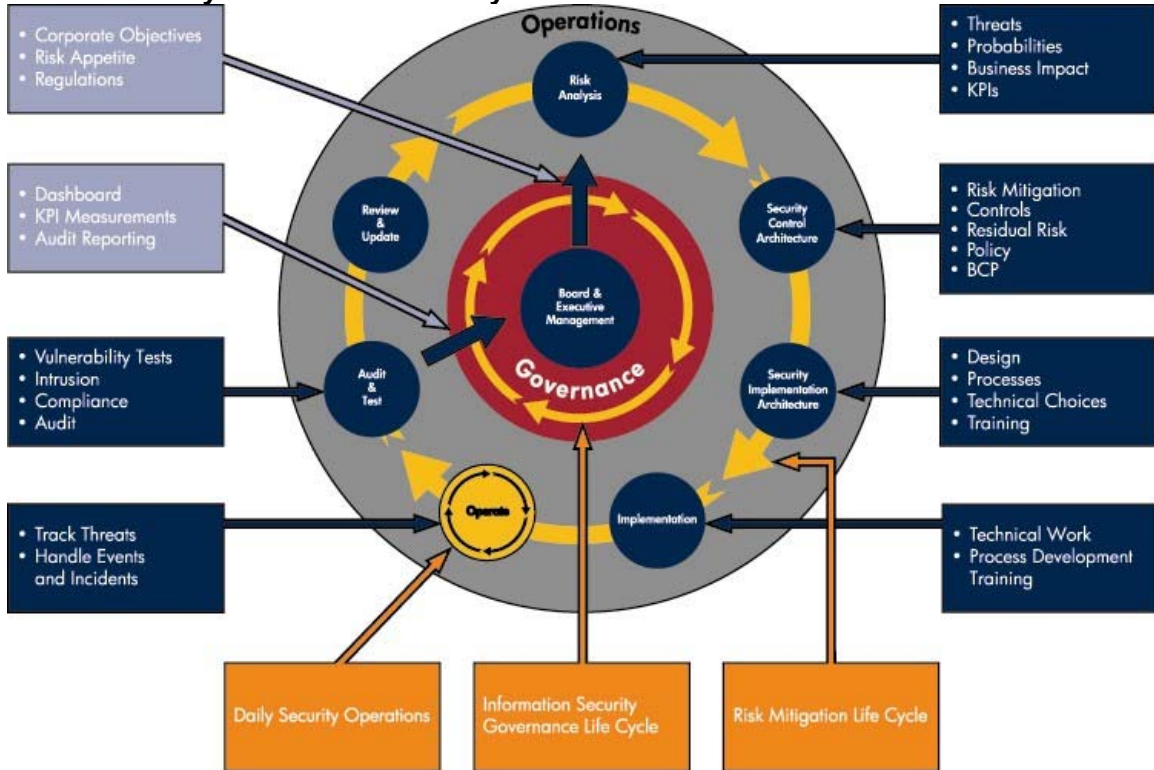


Figure 6 - Information Security Life Cycle Architecture

Successful security relies primarily on people and process:

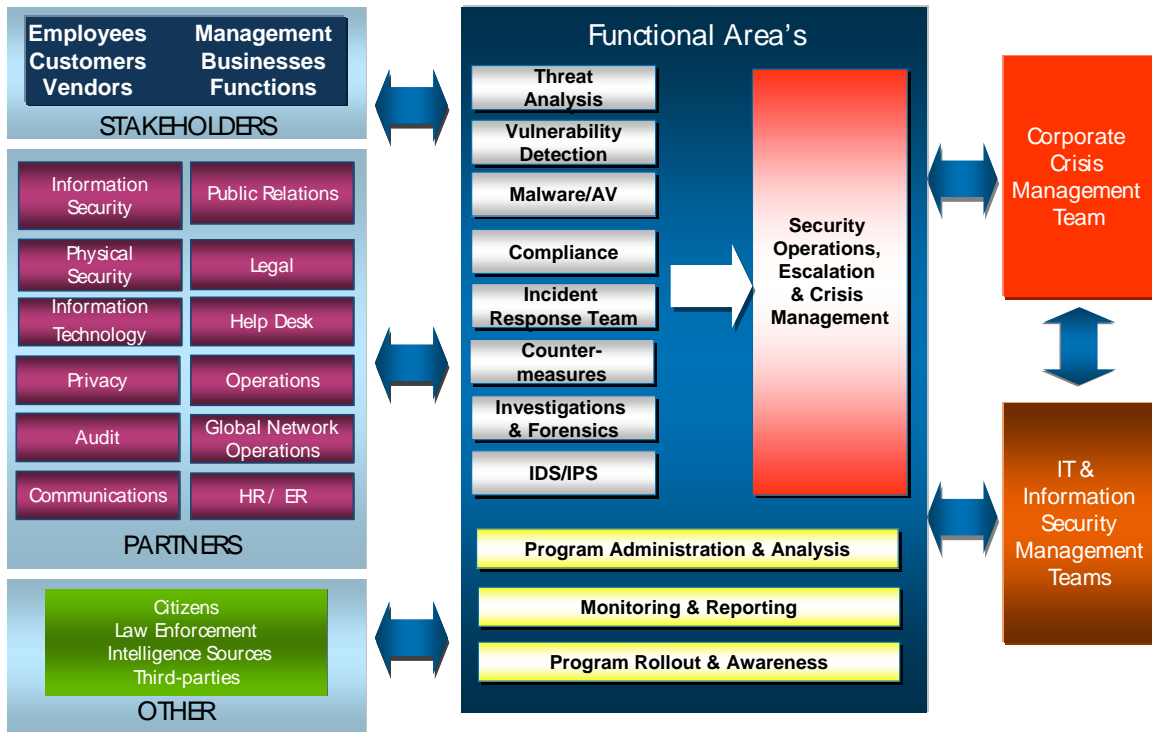


Figure 7 - Operational Security Management Information Flow

5.2 Physical Domain Model(s)

The diagram below shows what a typical security management technical architecture includes. It also shows how the common security and systems management tools integrate to provide a richer service management view of the enterprise.

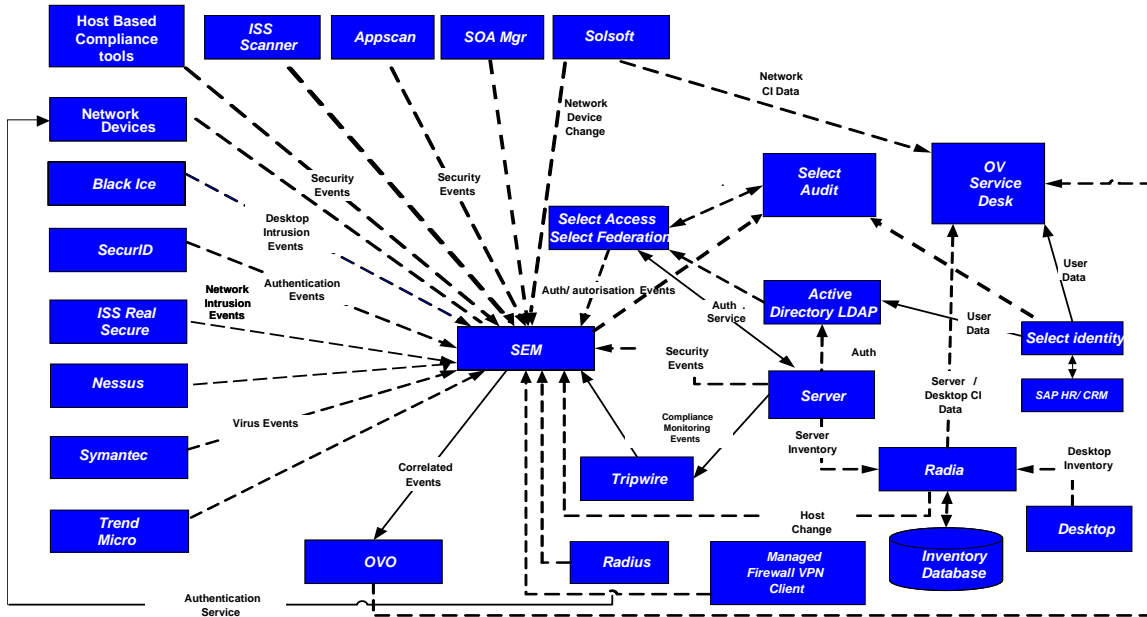


Figure 8 - Security Management Technical Architecture

5.3 Enterprise Security Domain Roadmap

Enterprises can rate their security at one of five levels:

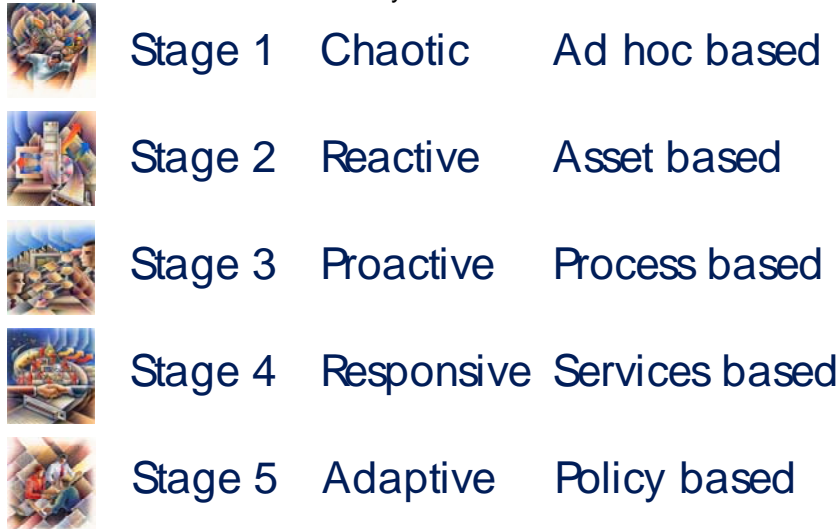


Figure 9 - Security maturity

Stage 1 – Chaotic

- Security team acts autocratically and in isolation, largely ignored by the rest of the business

- Investment in some preventative and detective security technologies
- Security policy in place but generally ignored
- Lack of business awareness and importance and value of security
- Pressure to reduce budget
- Security breaches often unreported

Stage 2 – Reactive

- Team organised around technical platforms, skill sets and functions in stove pipe fashion
- Asset cost minimisation through consolidation, utilisation control and life cycle management
- Cost efficiency of assets and people
- Lack of co-ordination and end to end accountability for service results
- Low service predictability and quality
- Large efforts for unanticipated situations
- Growing awareness to do something about security at the enterprise level

Stage 3 – Proactive

- Optimisation of end to end processes and costs (IDM, Vulnerability, SIEM, IPS, NAC etc)
- IT processes are implemented, measured and monitored, costs captured, resources co-ordinated
- Process goals and workflows dictate organisational design
- Security Program office and LOB representatives with permanently integrated, multidisciplinary teams
- Best practice process models such as ISO17799, ITIL
- Security strategy & architecture in place

Stage 4 – Responsive

- Shared services focus on optimising internal customer experience (IdM, virus protection etc)
- People, process and technology integrated
- Team based organisation
- Defined price-based service portfolio, partnering where weak
- Achieve contractually negotiated cost and quality goals
- Enterprise sees security as a driver of business process improvement or operational enhancement
- Integration of security management with overall IT management

Stage 5 – Adaptive

- Security and the business are fused
- Security is leveraged for external competitive advantage or to contribute revenue
- Can explicitly quantify financial contribution to revenue
- Mature service policy management
- Real time infrastructure with continuous process improvement with automated service levels tied to business
- True service agility, instantaneous response to business policy change
- Security governance adds automation to process of balancing capacity demand and resources between services
- Resources optimised and balanced against risk exposure

Security Competence	Chaotic	Reactive	Proactive	Supportive	Adaptive
Strategy	No clear security strategy	Strategy definition implicit but not documented ?	Strategy defined and attempts to define security issues	Clear security strategy articulated	Security strategy is aligned to business strategy
Governance Style	Anarchy ?	Duopoly	Federal	IT monarchy	Business Monarchy
Policies & Procedures	Sporadic if at all documented	Developed in response to specific incidents or problems	Developed ad hoc	ISO 17799 compliant/accredited ?	Adapted to changes in business environment
Architecture	Product-led ?	Architecture trails product implementation	Security architecture defined ahead of product selection	Security architecture integrates with IT architecture	Security architecture supports business strategy
Awareness & Culture	Awareness limited to IT staff	Awareness reinforced after specific breaches	Security awareness is part of all employment induction process ?	Awareness reinforced and culture assessed	Information security respected throughout the business
Technology deployment	Security products deployed on an ad hoc basis ?	Products deployed as remedial action to intrusion attempts	Security products deployed to create a rigid perimeter defense	Wide range of products deployed to cater to perceived threats	Products aligned to security architecture before deployment
Audit Monitoring & investigation	Non-existent; no audit trails are maintained to investigate	Compliance work is reactive to audit or security breaches ?	Audit and transaction data exists; investigation processes established	Audit and investigation processes are tested and optimized	Monitoring exists at the level of individual transactions
Resource Consumption and Value Demonstration	Minimal resources deployed	Basic spending on security technology with ROI ?	Business-unit-led spending on security; overall spending uncertain	Significant resources applied to security; security budget identified	Spending optimized and based on architecture; investment benefits balanced against cost

Figure 10 - Security maturity scorecard

6.0 Making it Happen

6.1 Technology Choices

With the information available, it is not possible to formulate a detailed architecture for the British Council. However, some tools should be considered mandatory for any successful security architecture. Examples include:

6.1.1 Security Incident Cost Calculator

Incident Management Program Per Incident Cost					
Instructions - Please fill in all fields highlighted in yellow.					
	Total	Totals by System Administrator			
		AP	Japan	EMEA	Latin America
Productivity Loss					
# of Servers Affected					
Average # of Hours of Server Downtime					
Average # of Users on Server During This Time					
# of Clients or PCs Affected					
Average # of Hours of Client or PC Downtime					
Average # of Users on Clients or PCs During This Time					
# of Employees Reading Messaging					
# of Hours Reading Messaging per Employee					
# of Employees Required to Perform Actions					
# of Hours Implementing Required Actions per Employee					
Hourly Rate per Employee					
Productivity Loss Subtotal	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!
Call Center Costs					
# of Support Calls	0				
Average Length of Call (in Hours)	0				
Cost per Call or Hour					

Figure 11 - Security Incident Cost Calculator

According to figures provided by the Worldwide Security Manager, the British Council recorded 96 security incidents in the two-year period up to April 7th 2008. It is noted that the impacts (financial, reputation, etc) of these incidents **are not known**; the WSM stated that it has proved too difficult to determine the actual costs.

Predicting the cost and probability of incidents is key to ensuring that any security measures are commensurate with the risk. The accuracy of these predictions can be improved by recording the actual costs of incidents should they occur.

There are many ways for any business to go offline: human error, power outages, security & service attacks, and of course natural and man-made disasters. In addition, it is not just servers or applications, the entire availability continuum that must be addressed. A critical aspect of any enterprises' business continuity planning is security.

Know your downtime cost: per hour, per day, per Business Unit...

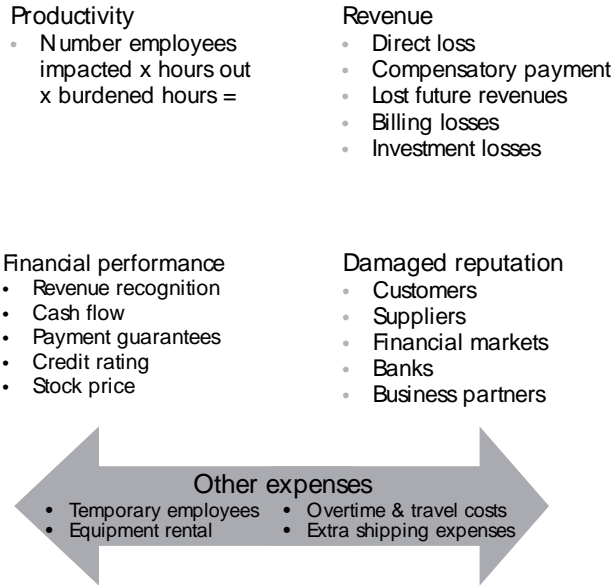


Figure 12 - Calculating downtime costs

6.1.2 Risk Assessment Matrix

A Risk Assessment Matrix provides a quick and consistent way to evaluate the risk severity of an information security threat, vulnerability or incident. It standardises escalation triggers, thresholds and actions across the Incident Management Program.

The Risk Assessment Matrix serves as a strong guideline for the initiation of a crisis or escalation and contains a series of metrics to help users identify the level of escalation. Scores are assigned in the areas of:

- The likelihood of an information security threat, vulnerability, or incident impacting the IT Infrastructure and
- The potential impact if the threat, vulnerability, or incident begins to affect the IT Infrastructure (including, but not limited to brand, financials, employees, customers, data/information loss, etc.)

Since the Council already has the Business Risk Management Framework, all that is needed is to apply the Council's adopted risk methodology mapping, *in detail*, to the areas of information security. This will ensure that the bulk of the critical decisions that need making during the pressure of an incident have already been made in the relative calm of an advanced planning session.

6.1.3 Crisis Management Manual

The Crisis Management Manual is a tool to assist on-call crisis managers in the event of an Information Security related crisis.

The Manual creates a standard process for managing high-profile incidents to ensure an immediate, appropriate, and consistent response to a geographic or worldwide crisis. This enables the Crisis Manager to take control of the crisis environment and manage the flow of information to protect the organisation most effectively.

In addition to aiding the Crisis Manager, the Manual contains tools, templates, flow charts, checklists and processes and outlines the responsibilities of other critical parties in the management of a crisis.

It is comparable with the Disaster Manual that is produced as part of an organisation's Disaster Planning program.

6.1.4 Incident Management Handbook

The Incident Management Handbook is a tool utilised by all members of the Incident Management Program. It contains all job descriptions, roles and responsibilities, processes and tool documentation for each of the Program components.

The Handbook provides a standard, easily accessible repository for securing all-important Program documentation that lends consistency and stability to the IM Program.

The Handbook is primarily utilised in a virtual manner with all documents undergoing regular scheduled review and update

6.2 Key Organisation Processes

The key organisational processes required are listed below:

- Risk Analysis and Management process
- Anti-virus process management process
- Patch management process (see the *Systems Management Domain Roadmap*)
- Security program rollout and awareness
- Security program administration and analysis process
- Threat analysis and response process
- Vulnerability detection process
- Escalation and crisis management process
- Security Architecture process
- Intrusion detection and response process
- Information security incident response process
- Investigation process

6.3 Resources and Skills, Provision Assumptions

The first and final defence to an organisation is people and hence the security organisation is a key piece of any security ecosystem.

Most of the capabilities require staff with specialist skills. While all the skills fall under the umbrella heading of “security”, it would be highly unusual to fulfil all roles with staff trained in all areas.

Resourcing all of the capabilities identified in 4.4 above, especially 4.4.4 would be a major undertaking. Indeed not all organisations can justify, *following a careful risk-based assessment of their assets*, implementing all of the capabilities.

Some capabilities can be outsourced, as part of “business as usual” activities. The Council already does this in part, with some third parties supposedly providing security facilities as part of their wider contracts, and some providing specialist “bureau” services, such as Message Labs’ anti virus capability.

Some capabilities, such as detailed forensic investigation, are (hopefully!) only required infrequently. They require highly specialist skills, and it is unlikely to be cost effective for the Council to develop and maintain such skills in-house. Therefore, the Council is advised to establish a relationship with a dedicated third party service provider, **before** such services are required.

Upon creation, an Information Security organisation must use the following guiding principles. These principles come initially from best practice but are also now being enshrined in various legislation.

1. Board must take ultimate responsibility; it is not a defence for someone to say that they did not know what was happening. Board member must be ultimately responsible for the Council’s assets and actions, they can delegate authority but not responsibility, therefore security must report directly into the board.
2. Must be empowered; The Chief Security Officer (CSO) must be empowered to effect change and direct people throughout the organisation, too often in the organisational structure has a CSO been a peer to other managerial positions within an organisation and has not had the power to make change in other area’s of the business. Even though the CSO should be empowered, the key to success is influence not authority.
3. Independent of Audit and IT; Security must be kept separate from Audit and IT functions to resolve conflict of interest issues which may occur. It is not appropriate to have a team policing itself.
4. Covers all business assets; usually information security is seen as an IT function. This is not so and it should be integrated with but not limited to entities like physical security, crisis management and business continuity. This is to ensure that that the information security organisation understands the impact of an incident on the business operation and the financial consequences.
5. Segregate of duties; Security duties must be segregated to stop collusion, which may cover up an incident or enable parties to carry out actions purposefully, which are against Council policy.

Figure 13 below describes a typical security organisation.

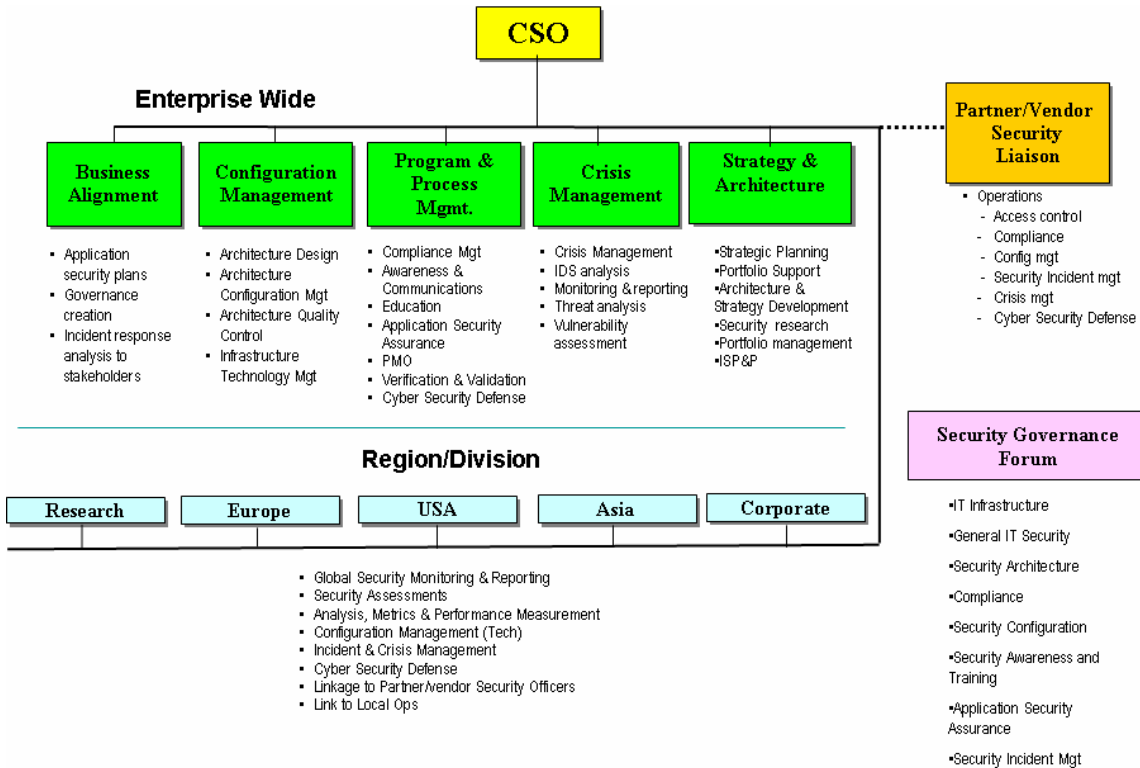


Figure 13 - Typical Security Organisation Structure

6.4 Milestones and Deadlines

In security, more than any other domain, there is no fixed future target state. There is instead the ongoing arms race for continual improvements in security, as new vulnerabilities and attacks are discovered and risks continue to morph.

What are presented here are some suggestions for the British Council to consider, taking into account the immediate, short and medium term goals of similar organisations.

For immediate consideration:

1. Ensure that risk assessments are up to date **and** readily available to authorised personnel. Clearly, the information is commercially sensitive, and must be protected. Use the risk assessments to prioritise security reviews of the different business units and underlying IT infrastructure, whether managed in-house or outsourced to a 3rd party.
2. Ensure that external parties fulfil their security obligations. In particular, security reports must be provided to the Council.

3. Ensure that the Worldwide Security manager is involved in the review of criteria and selection process of any third party service providers that affect security⁶.
4. Reduce the backlog of critical and security patches. It is suggested that:
 - Within one week of release, patches are tested on the existing test systems
 - If no incompatibilities are found within one week of testing, these patches are rolled out to designated pilot offices. The pilot offices should represent a broad sampling (10%) of all office types and regions. Systems in these offices should have their operating system and application partitions “cloned”⁷ before patches are applied, to facilitate speedy regression should any incompatibilities be discovered.
 - If no incompatibilities are found within one month of real-world use by the pilot offices, the patches should be rolled out across the whole enterprise.Such a scheme would reduce the window of exposure down to 6 weeks.

For short-term consideration, i.e. within the next 12 months:

5. Establish centralised security monitoring of systems managed in-house. This should include automated log-file analysis, with a view to reducing the burden on the WSM.
6. WSM and his team should have read-only access to the outsourced third parties’ security incident monitoring consoles, so that events can be monitored in real-time. This would be analogous to the Service Delivery Manager having read-only access to the outsourced third parties’ Service Management dashboards.
7. The GIS architecture team should ensure that security skills are available within or to development and project teams. For instance, developers should be trained on secure coding practices.
8. Plan and execute security reviews of the key business units and infrastructure components as identified during the risk analysis exercises. Use readily available industry-standard security benchmarks such as [Ref 9] for quick wins.
9. Consider the use of automated file-system integrity assurance mechanisms, such as Tripwire, on key systems.
10. Consider the use of automated policy compliance checking tools such as Enterprise Security Manager.
11. Enforce the governance around the use of external third party web hosting companies.

For medium-term consideration:

12. The tone of the Information Security Policy should be modified so that it is more proscriptive rather than suggestive. The current wording might provide too much opportunity for legal challenges should it need to be used to prosecute offenders.

⁶ Yes, everything impacts security ☺

⁷ E.g. using Norton “Ghost”, Acronis “True Image” or VM snapshots, etc

6.5 Domain Strategic Roadmap

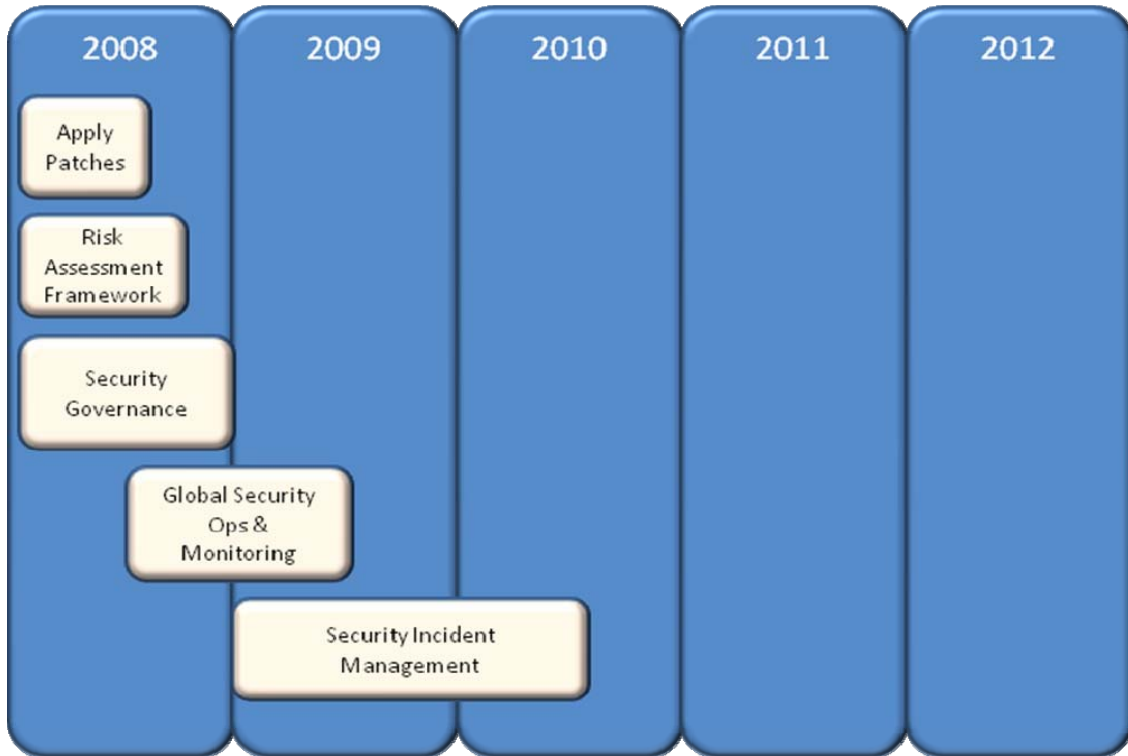


Figure 14 - Security Domain Strategic Roadmap

6.5.1 Step 1 - Establish Risk Assessment Framework

Provide a mechanism to assess the British Council's security requirements that can drive the business and IT security architecture.

6.5.2 Step 2 - Establish Security Architecture Governance

Put into action strong governance to ensure implementation of the IT security architecture. Ensure that all new solutions are compliant with security requirements, standards and policies. Review all existing solution against the architecture and carry out remedial action where required.

6.5.3 Step 3 - Set up Global Security Operations & Monitoring

Set up the mechanism to monitor security so that there is a known British Council security state at all times.

6.5.4 Step 4 - Introduce Security Incident Management

Introduce *Security Incident Management Process*; ensure that this is done in harmony with the wider IT service management initiatives.

7.0 Appendix 1 - Principles Guiding the Security Domain

7.1 Business Principles

Business Principle 4 - Security Strategy

7.2 Functional Principles

Functional Principle 6 - Legal and Regulatory Requirements

Functional Principle 7 - Confidentiality, Integrity and Availability of Data and Systems

Functional Principle 8 - Security Policy

Functional Principle 9 - Information Quality

Functional Principle 10 - Business Continuity

7.3 Technical Principles

Technical Principle 4 - Industry Standards

Technical Principle 5 - Security Standards

Technical Principle 6 - Solution Characteristics

7.4 Governance Principles

Governance Principle 4 - Enterprise architecture is business driven

Governance Principle 5 - Architectural values are to be publicised

Governance Principle 6 - Architecture efforts must be unified across the Enterprise

8.0 Appendix 2 - References

This following are referenced within this document:

Ref	Title
Ref 1	“Risk & Opportunity Identification (UK) (Element 1 of BRMF)” Version 4, August 2007 Business Process Development & Training Team
Ref 2	Information Security Policy March 2008 Terry Pipe
Ref 3	Platform Domain Roadmap April 2008 Mark Cooper (HP)
Ref 4	Systems Management Domain Roadmap April 2008 Mark Cooper (HP)
Ref 5	UK Schedule 2 – The Services and Deliverables Outsourcing contract with LogicaCMG v7
Ref 6	Schedule 1 –Services Outsourcing contract with Global Crossing
Ref 7	SAP support contract with HP
Ref 8	Business Risk Management Framework
Ref 9	Security assessment and scoring tools Centre for Internet Security http://www.cisecurity.org/