Information
Security
Forum

Information security for external suppliers: A common baseline

Executive overview

Introduction

This Executive Overview highlights the key findings from the ISF's report ***ISF Information security for external suppliers: A common baseline***. Over 310 professionals from ISF Member organisations examined how information security could be enhanced in the management of external suppliers (a revised term replacing third parties – see back page for a definition). The overview outlines the key findings of the project, presents selected responses from a Member questionnaire on this topic and the baseline information security arrangements for external suppliers.

The need for a baseline

83% of respondents outsource functions such as IT, HR or payroll

Organisations now use external suppliers in many ways, such as: interacting with customers on their behalf; writing software; running business processes; and providing IT and HR functions.

Many of these external suppliers deal with sensitive, confidential or personally identifiable information – and its accidental or deliberate loss could damage both the external supplier and the organisation. As a result, organisations and external suppliers need assurance that:

- information security is being taken seriously
- key risks are being addressed
- information security arrangements are implemented and effective.

Who would use the baseline?

85% of respondents would apply the baseline to the external suppliers which are critical to their business

ISF Members want a set of baseline arrangements they can use in their business relationships. Such a baseline would move the focus away from fundamentals (ie the baseline) and allow the identification and specification of additional controls an external supplier should implement.

A baseline for all external suppliers

90% of respondents agree that a key objective is to define the baseline security arrangements applicable to all external suppliers

The ISF has created the baseline arrangements, using inputs such as the ISF's ***21 Guidelines for information security***, good practice drawn from ISF Members, workshop analysis and previous ISF work in this area, notably the ***Third Party Security Assessment Tool*** and the ***Information security in third party relationship management*** project.

The common baseline arrangements cover approximately 80% of the information security requirements acquiring organisations ask their external suppliers to implement. The other (approximately) 20% are usually specific to the acquirer, or the sector or jurisdiction in which the acquirer operates.

The baseline arrangements are divided into the eight ***ISF Benchmark*** groups, namely:

- Governance, risk and compliance
- System management
- Access management
- Security monitoring and response
- Network connections
- Electronic communications
- Business control
- System development.

The baseline arrangements are ***mandatory*** – that is, an external supplier must be able to demonstrate it meets all of them.

Creating a global standard: working with ISO

87% of respondents agree that this work should form the basis of a global ISO standard

The ISF has successfully presented this work to the ISO SC27 committee, which is responsible for the ISO 27000 series of standards for information security.

This success may result in the acceptance of this ISF work as part of a new, revised standard termed ISO/IEC 27036: Information technology – Security techniques – Information Security for Supplier Relationships. This may open new ways in which the ISF can deepen its relationship with ISO and contribute to the creation of ISO/IEC 27036.

Categorising external suppliers

Understanding the relationship between an acquirer and the external supplier is a key step to identifying the additional information security arrangements required. A structured approach based around a business and security perspective has been developed, using an external supplier assessment questionnaire and a business impact assessment to categorise external suppliers. This assessment and categorisation provides a high-level business and security perspective of the external supplier.

		Assessment question	Yes / No
External supplier organisation	Size of external supplier	Is the external supplier smaller than our organisation in terms of revenue?	
	Supplier history	Is the external supplier a well known company in the market space?	
	Supplier reputation	Does the external supplier have a good reputation in the market, ie there are no known major issues with other organisations?	
	Business relationship	Has the external supplier previously worked with our organisation?	
		Is the external supplier working with our organisation at present?	
	Maturity of external supplier service offering	Has the external supplier previously provided, managed or delivered this service to our or another organisation?	
	Location of external supplier	Does the external supplier have a physical presence in the same geographical regions (eg county, state or nation) as our organisation?	
	Disputes	Have all outstanding contractual, legal or other disputes between our organisation and the external supplier been resolved?	
	Competition	Is the external supplier providing services to a major competitor?	
	Governing jurisdiction	Is the contract or SLA governed by the legal jurisdiction of our choice?	
	Non-Disclosure Agreement(s)	Is a non-disclosure agreement / confidentiality clause in place to cover the contracting process and external supplier staff?	

The external supplier assessment provides a business and security perspective of a supplier, covering areas such as:

- characteristics of the external supplier
- contract
- security
- compliance

Impact type		Potential impact on our organisation should the external supplier have a breach or loss of		
		Confidentiality	Integrity	Availability
Financial	Loss of sales, orders or contracts	H	L	M
	Loss of tangible assets	H	L	L
	Penalties/legal liabilities	L	M	M
	Unforeseen costs	VH	M	L
	Depressed share price	VH	L	M
Operational	Loss of management control	H	H	H
	Loss of competitiveness	VH	H	M
	New ventures held up	M	L	L
	Breach of operating standards	L	M	VL
Customer-related	Delayed deliveries to customers or clients	H	H	VH
	Loss of customers or clients	M	H	H
	Loss of confidence by key institutions	VL	M	L
	Damage to reputation	H	VH	VH
Employee-related	Reduction in staff morale/productivity	L	L	VH
	Injury or death	VL	VL	VL
Externa plier-related	Reduction in quality of service provided to acquiring organisation's customers	H	M	H
	Loss, either maliciously or accidentally, of acquirer's information	H	M	H
	Failure of external supplier's Business Continuity/Disaster Recovery processes	L	M	VH
	Breach of international data transfer agreements	H	L	L
	Breach of Intellectual Property Rights	H	H	VL
	Number of impact types answered with Very High or High (out of 20)	12	6	8

The business impact assessment examines the impact on the acquirer should the external supplier have a breach of confidentiality, integrity or loss of availability of information either through accidental, deliberate or natural causes

The results from the external supplier assessment questionnaire and the business impact assessment can be combined and used to categorise the external suppliers and hence indicate whether additional information security requirements may be required.

Common baseline information security arrangements

These arrangements are based on the *ISF's 21 Guidelines for information security* and aligned to the *ISF Benchmark*. To address particular concerns when working with external suppliers, 11 specific controls (which are at a more detailed level than the baseline arrangements) are highlighted in colour in the following table.

Domain	Baseline information security arrangement	What the external supplier needs to do
Governance, risk and compliance	Information security framework	Establish, maintain and monitor an information security governance framework
	Information security policy	Develop and distribute a comprehensive, approved information security policy to all individuals with access to the organisation's information and systems
	Awareness/education	Establish an information security awareness and behaviour change programme, supported by a range of education/training activities
	Information risk management	Undertake information risk management for key aspects of the service, on a regular basis, in a rigorous and consistent manner, using a structured methodology
	Identification and protection of information that is commercial, sensitive, regulated or personal in nature	Apply an approved method for identifying, maintaining and protecting information such as trade secrets, Intellectual Property, financial, defence-related, food and drug, or personally identifiable information
	Accountability/ownership	Assign ownership and responsibility for particular information and systems to designated individuals who have the required skills, tools and authority
System management	Purchase of hardware and software	Acquire only secure, approved hardware and software (eg purchased from an approved list, subject to a security evaluation and recorded in an inventory)
	Robust resilient design	Design and operate robust, resilient systems that can cope with current and predicted levels of usage, are supported by alternative facilities and incorporate information security requirements
	Separation of primary functions	Deploy servers that implement only one primary function (eg web server, transaction server or database servers should be implemented on separate servers)
	Separation of client databases/ data sets	Separate, both physically and logically, data from one client from that of other clients
	Configuration and security settings	Configure systems in a consistent, accurate manner and apply and monitor approved security settings
	Input/process/output validation	Validate information entered into, processed by and output from business applications and verify that it has not been subject to unauthorised change
	Physical protection	Protect IT facilities equipment and services against malicious attack, accidental damage, natural hazards and unauthorised physical access
	Control of portable storage devices	Restrict the use of unapproved devices and disable the ability to copy data to them
Access management	Segregation of duties	Segregate duties and areas of responsibility to reduce the risk of accidental or deliberate system or application misuse
	Identity and access management	Implement a consistent identity and access management approach that provides effective user administration, identification, authentication and authorisation mechanisms
	Access control	Restrict access to designated information and systems to specified individuals or roles in external suppliers (eg customers, suppliers and business partners) who have been authorised and are subject to agreed security requirements in an approved contract
	Privileged user management	Use strong authentication, force regular password changes and log, monitor and review the activities of privileged users (eg superusers, administrators, DBAs, or people who have access to sensitive or critical information)
Security monitoring and response	Continuous monitoring of systems and networks	Perform continuous monitoring of designated systems and networks, employ intrusion detectio
	Malware protection	Deploy comprehensive, up-to-date malware handling malware infecti
	Patch management	
	C	
		ystems that includes identification, y incidents
		gs and other appropriate material
N co		Design and operate robust, resilient networks that can cope with current and predicted levels of traffic, are supported by alternative facilities, incorporate firewalls and restrict network access to authorised individuals
	Control of network access/ connectivity	Restrict connections to the Internet, customers and external suppliers and, where possible, separate those connections
Electronic communications	Protection of electronic communications	Protect electronic communication systems (eg e-mail, instant messaging and VoIP) by setting policy for their use, configuring security settings, performing capacity planning and hardening the supporting infrastructure
	Use of cryptographic solutions	Apply approved, documented cryptographic solutions, supported by effective cryptographic key management
Business control	Sub-contractor management	Restrict access to designated information and systems to sub-contractors and business partners who have been authorised and are subject to agreed security requirements in an approved contract
	Security audit and review	Conduct thorough, independent and regular security audits / reviews and publish the results both internally and for the acquirer
	Business continuity	Have a business continuity plan that is supported by alternative processing facilities and tested regularly using simulations of the live environment
System development	System Development Life Cycle methodology	Develop systems using a structured and approved system development methodology that ensures information security requirements are considered as part of the process, and consequently defined, documented and met

External supplier baseline maturity model

The baseline arrangements provide statements of capability for an external supplier, which can be evaluated by a simple 'Yes' or 'No'. To enhance the utility of the arrangements, a maturity model has been developed, in which each arrangement has five levels of capability, ranging from 'non-existent' to 'optimised'. Members can use the maturity model to assess the capability of, or set a minimum capability to be attained by, an external supplier for each baseline arrangement.

Defining external suppliers

The term 'third party' has been in use for a number of years, yet definitions are often obscure or unhelpful. To clear this confusion, the ISF has replaced the term with that of 'external suppliers'. Using this term removes any legal issues or confusion and brings ISF terminology into line with that of other organisations.

An external supplier is defined as '***an organisation that provides goods or services to an acquiring organisation***'.

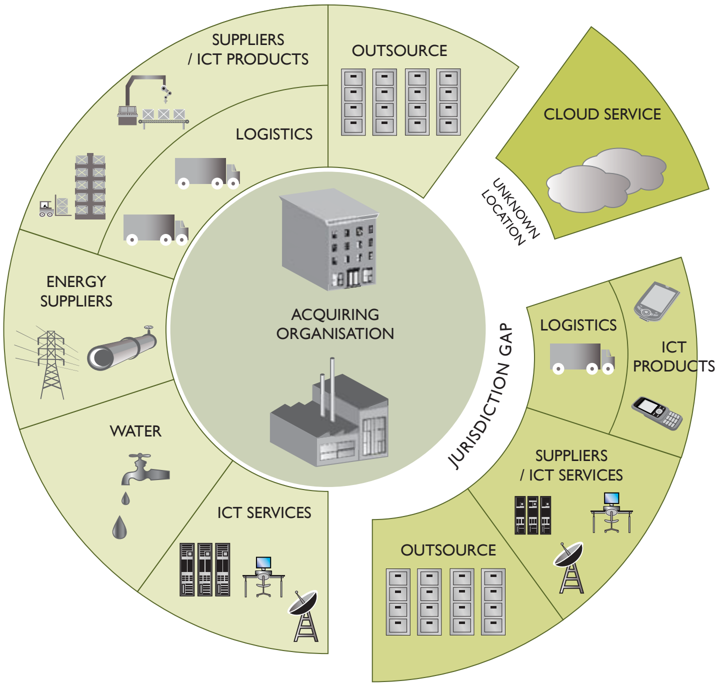
For the purpose of the report, the scope includes – but is not limited to – external suppliers: Outsourcers, Information and Telecommunication Technology (ICT) service providers, ICT product providers and Utilities. They are defined in the table below.

	Outsourcers	Information and Telecommunication Technology services	Information and Telecommunication Technology products	Utilities
What the external suppliers do	Business Process Outsourcing (BPO) Knowledge Process Outsourcing (KPO) IT/Data Centre management and operation Specific activities (eg payroll)	Web-hosting Cloud service providers (Software as a Service, Platform as a Service, Infrastructure as a Service) Internet Service Providers (ISP)	Provide software, middleware and hardware	Gas, water, electricity, fixed and mobile telecoms, postal services
Location of external supplier with respect to acquirer	Same geographical region (eg the same country in the same continent) OR Different geographical region (eg different country, different continent) (sometimes termed 'offshore outsourcers' or offshorers)	Same geographical region (eg the same country in the same continent) OR Different geographical region (eg different country, different continent)	Same geographical region (eg the same country in the same continent) OR Different geographical region (eg different country, different continent)	Typically the same geographical region

Organisations sit in the middle of a complex web of relationships. Typically, an organisation will work with many external suppliers such as IT outsourcers to bankers, consultants to cloud service providers and lawyers to Internet service providers. The diagram (see right) illustrates these relationships at a high level – and also highlights the fact that relationships can cross jurisdiction and location.

For the purposes of this report, the following are out of scope, as information security will be addressed in a different manner:

- Organisational and individual customers
- Individual external suppliers (eg individuals working for the acquirer under a contract)
- Governments and statutory authorities (such as regulators)
- Infrastructure providers (eg external suppliers that build or provide facilities such as roads, airports and ports).



Warning

This document is confidential and purely for the attention of and use by organisations that are Members of the Information Security Forum (ISF). If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on isfinfo@securityforum.org or on +44 (0)20 7213 1745. Any storage or use of this document by organisations which are not Members of the ISF is not permitted and strictly prohibited.

This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

The Information Security Forum is an independent, not-for-profit association of leading organisations dedicated to clarifying and resolving key issues in information security and developing security solutions that meet the business needs of its Members.