

FRAMEWORK



CPI·RISC

**Continuous Process Improvement–
Risk, Information Security, and Compliance**

The pragmatic, business-oriented, standards-based methodology for managing information risk.

CPI-RISC Information Risk Framework
v1.1, Sep 2010

Jim Herbeck, CISSP, CISA
Managing Partner, NOUVEL Strategies
Member of Faculty, the SANS Institute
Advisory Board Member, CCSIE

Information Risk Framework Introduction

The CPI-RISC¹ Information Risk Framework (IRF) was developed as a tool to assess and treat information- and IT-related risks. The IRF is based on ISO 27001², ISO 27002³, and the SANS Institute 20 Critical Security Controls⁴. Additionally, the IRF is built on the premise that information risk management is an organizational issue, not exclusively an IT issue.

There are three potential problems with existing risk management and information security standards:

1. IT-oriented structure: standards are written and structured for information security or IT professionals. This structure is inefficient for non-IT professionals to decipher and implement.
2. Complexity: standards are often lengthy and complex. For example, ISO 27002 has 133 controls organized into 12 sections in 128 pages. As a result of the length and complexity, standards can be difficult to understand by non-technical business managers.
3. Lack of prioritization: standards typically don't offer concrete guidance in how to prioritize risk. In order to create an effective security program, it is essential to be able to identify risks with the highest priority.

The CPI-RISC IRF provides a sensible solution to these problems:

1. Business-oriented structure: the IRF is written and organized for non-technical business managers. The framework is organized into 8 different business functions that cross the entire organization:
 - Management (MGT)
 - Personnel (PER)
 - Legal (LEG)
 - Facilities (FAC)
 - Finance (FIN)
 - Information Technology: Application Development (ITA)
 - Purchasing (PUR)
 - Information Technology: Services (ITS)
2. Simplified: the IRF defines 33 risk areas, categorized into 8 business functions in 12 pages. Information risk areas for most business functions are defined on a single page.
3. Prioritized: the IRF specifies risk priority levels for each risk area, making it more efficient to identify high risks:
 - A (High Priority)
 - B (Medium Priority)
 - C (Low Priority)

Used with the CPI-RISC Methodology, the CPI-RISC IRF can be part of an efficient and effective risk assessment program.

1 The Continuous Process Improvement–Risk, Information Security, and Compliance (CPI-RISC™) methodology is a pragmatic, standards-based, business-oriented approach to information security. CPI-RISC was developed by NOUVEL Strategies and is available for use under the Creative Commons cc-by-sa license. <http://nouvelstrategies.com/E/CPI-RISC.html>

2 ISO/IEC 27001:2005: Information technology–Security techniques–Information security management systems–Requirements. A widely used information security standard.

3 ISO/IEC 27002:2005: Information technology–Security techniques–Code of practice for information security management. A well-respected definition of best practice for information security.

4 The SANS Institute 20 Critical Security Controls were defined by a government/industry consortium to help organizations focus their efforts on security controls that block known attacks. <http://www.sans.org/critical-security-controls/>

Information Risk Framework Summary

The CPI-RISC Information Risk Framework (IRF) defines 33 risk areas with risk priority levels, categorized into 8 business functions¹.

Management risk

MGT1	Information risk management	A
MGT2	Information security management	A
MGT3	Compliance management	A
MGT4	Business continuity risk	A
MGT5	Security organization risk	C

Legal risk

LEG1	Legal, regulatory, and contractual compliance risk	A
-------------	--	----------

Finance risk

FIN1	Financial fraud risk	A
FIN2	Information access control risk	A

Purchasing risk

PUR1	Third party risk	A
PUR2	Information asset management risk	A
PUR3	Software license management risk	B

Personnel risk

PER1	Pre-employment risk	A
PER2	Employee risk	B
PER3	Post-employment risk	B

Facilities risk

FAC1	Site-related physical risk	A
FAC2	Equipment-related physical risk	B
FAC3	Workspace-related physical risk	C

IT application development risk

ITA1	Development process risk	A
ITA2	Application-related risk	B

IT service risk

ITS1	Data center risk	A
ITS2	Operational integrity and availability risk	A
ITS3	Disaster-related risk	A
ITS4	Network-related risk	A
ITS5	System-related risk	A
ITS6	Identity-related risk	A
ITS7	Malicious software risk	A
ITS8	Mobile worker-related risk	A
ITS9	Third party service management risk	B
ITS10	Message service-related risk	B
ITS11	Web/eCommerce-related risk	B
ITS12	Security incident-related risk	B
ITS13	Storage media-related risk	B
ITS14	Service planning-related risk	C

¹ The CPI-RISC Methodology specifies that organizations should customize and adapt the business functions, risk areas, and risk priority levels of the CPI-RISC IRF as appropriate.

Management risk

Information risk areas that are the responsibility of general management.

MGT1	Information risk management	A
	Overall risk associated with not assessing and treating information risk. Risk controls include: - performing periodic information- and IT-related risk assessments. - developing and approving risk treatment plan. Step 1 of CPI-RISC.	
	ISO 27001:2005 4.2.1d-h	
MGT2	Information security management	A
	Overall risk associated with not managing information security. Risk controls include: - developing and maintaining an information security policy that addresses the organization's information- and IT-related risks. - management support for information security. Step 2 of CPI-RISC.	
	ISO 27001:2005 A.5.1.1, A.5.1.2, A.6.1.1	
MGT3	Compliance management	A
	Overall risk associated with not auditing or assessing information security. Risk controls include: - performing periodic, independent reviews of information security. - using automated, technical assessment tools. Step 3 of CPI-RISC.	
	ISO 27001:2005 A.6.1.8, A.15.2.1, A.15.2.2; SANS CC10, CC17	
MGT4	Business continuity risk	A
	Risk of disruptive event negatively impacting business. Disruptive events could include natural disasters, severe weather, or labor disputes. Risk controls include: - developing and testing business continuity plans.	
	ISO 27001:2005 A.14.1.4, A.14.1.5	
MGT5	Security organization risk	C
	Risk of not being able to manage information- and IT-related risks due to a lack of organization and coordination. Risk controls include: - coordinating activities between different business functions. - defining information security responsibilities.	
	ISO 27001:2005 A.6.1.2, A.6.1.3	

LEGAL

Legal risk

Information risk areas that are the responsibility of the legal department.

LEG1	Legal, regulatory, and contractual compliance risk	A
	Risk of noncompliance with legal, regulatory, or contractual requirements for information security. Includes national laws as well as contractual obligations to customers. Risk controls include: <ul style="list-style-type: none">- verifying compliance with national laws and regulations.- verifying compliance with data protection and privacy law.- verifying compliance with legal requirements for records retention.- verifying compliance with contracts for services provided to customers.	
	ISO 27001:2005 A.6.2.2, A.15.1.1, A.15.1.3, A.15.1.4	

Finance risk

Information risk areas that are the responsibility of the finance department.

FIN1	Financial fraud risk	A
	Risk of financial fraud. Includes theft of money from the organization by manipulating finance-related processes. Risk controls include: <ul style="list-style-type: none"> - segregating duties and areas of responsibilities. - eliminating job duties that create a conflict of interest, particularly with finance-related jobs. 	
	ISO 27001:2005 A.10.1.3; SANS CC9	
FIN2	Information access control and management risk	A
	Risk of improper information access or modification. Risk controls include: <ul style="list-style-type: none"> - preventing unauthorized or unintentional access, modification, or misuse of information assets. - developing and enforcing an Access Control Policy and Acceptable Use Policy. - ongoing maintenance and monitoring of access and access rights. 	
	ISO 27001:2005 A.7.1.3. A.7.2.1, A.11.1.1, A.11.2.4	

Purchasing risk

Information risk areas that are the responsibility of the purchasing department.

PUR1	Third party risk	A
	<p>Risk of information assets being accidentally or maliciously compromised by third party service providers. Includes network service providers, IT support service providers, outsourced software development, and temp or contract workers provided by staffing agencies. Risk controls include:</p> <ul style="list-style-type: none"> - identifying risk areas with third party providers. - ensuring that third parties are contractually obligated to protect information assets. - addressing security with outsourced software development contracts. <p>ISO 27001:2005 A.6.2.1, A.6.2.3, A.12.5.5</p>	
PUR2	Information asset management risk	A
	<p>Risk of losing information assets by inadequate asset management. Risk controls include:</p> <ul style="list-style-type: none"> - maintaining a current inventory of all information assets and asset owners. - ensuring appropriate labeling and handling for sensitive information assets. <p>ISO 27001:2005 A.7.1.1, A.7.1.2, A.7.2.2; SANS CC1</p>	
PUR3	Software license management risk	B
	<p>Risk of unlicensed commercial software. Includes legal risk as well as availability risk (self-disabling software). Risk controls include:</p> <ul style="list-style-type: none"> - maintaining purchase records for all licensed software. - ensuring software is being used according to license agreements. <p>ISO 27001:2005 A.15.1.2; SANS CC2</p>	

PERSONNEL

Personnel risk

Information risk areas that are the responsibility of the personnel department.

PER1	Pre-employment risk	A
	Risk of hiring malicious employees who will compromise information assets. Risk controls include: <ul style="list-style-type: none">- defining security roles and responsibilities in job descriptions.- requiring signed confidentiality agreements.- requiring signed employment contracts.- performing background checks for sensitive positions. ISO 27001:2005 A.6.1.5, A.8.1.1, A.8.1.2, A.8.1.3	
PER2	Employee risk	B
	Risk of information assets being accidentally or maliciously compromised by employees. Risk controls include: <ul style="list-style-type: none">- awareness programs for new workers.- periodic awareness program updates for all workers.- periodic security training for workers with information security responsibilities. ISO 27001:2005 A.8.2.2; SANS CC20	
PER3	Post-employment risk	B
	Risk of terminated employees compromising information assets. Risk controls include: <ul style="list-style-type: none">- utilizing a formal worker termination procedure.- verifying information assets are returned.- verifying access rights are removed and user accounts are deleted. ISO 27001:2005 A.8.3.1, A.8.3.2, A.8.3.3	

FACILITIES

Facilities risk

Information risk areas that are the responsibility of the facilities department.

FAC1	Site-related physical risk	A
	<p>Risk of theft of information assets from buildings or business locations due to a lack of physical security. Risk controls include:</p> <ul style="list-style-type: none"> - defining a physical security perimeter. - installing and maintaining keyed or electronic door locks. - requiring workers and visitors to wear identification badges. - maintaining a physical or electronic access log. - protecting buildings or business locations from external and environmental threats, including fire, flood, earthquakes, and civil unrest. - ensuring delivery and loading areas are secure. 	
	ISO 27001:2005 A.9.1.1, A.9.1.2, A.9.1.4, A.9.1.6	
FAC2	Equipment-related risk	B
	<p>Risk of theft of workstations, laptops, or PDAs (or information from such devices) due to a lack of physical security. Risk controls include:</p> <ul style="list-style-type: none"> - preventing loss, damage, theft, or compromise of equipment. - ensuring that equipment leaves the premises via a formal process. - ensuring secure equipment disposal. 	
	ISO 27001:2005 A.9.2.1, A.9.2.6, A.9.2.7	
FAC3	Workspace-related risk	C
	<p>Risks due to theft of information from a work area. Risk controls include:</p> <ul style="list-style-type: none"> - protecting unattended equipment. - keeping desks and screens clear. 	
	ISO 27001:2005 A.11.3.2, A.11.3.3	

IT application development risk

Application development-related information risk areas that are the responsibility of the IT department.

ITA1	Development process risk	A
	Risk of security vulnerabilities in software due to a flawed software development process. Risk controls include: <ul style="list-style-type: none"> - analyzing security requirements for business systems. - using formal change control to manage the development process. - using a formal system acceptance process to document and test operational requirements of new systems. 	
	ISO 27001:2005 A.10.3.2, A.12.1.1, A.12.5.1	
ITA2	Application-related risk	B
	Risk of leaked information or incorrect results due to software flaws. Risk controls include: <ul style="list-style-type: none"> - detecting errors in input data. - preventing errors in output data. - utilizing cryptography to prevent the inadvertent disclosure of data. 	
	ISO 27001:2005 A.12.2.1, A.12.2.4, A.12.3.1; SANS CC7	

IT service risk

Service-related information risk areas that are the responsibility of the IT department.

ITS1	Data center risk	A
	<p>Risk of inability to use of server room or data center due to inadequate data center management. Risk controls include:</p> <ul style="list-style-type: none"> - locating data processing equipment in locations that are discreetly located and physically secure. - requiring management approval for all new data processing facilities. - ensuring adequate supporting utilities in data processing facilities. - ensuring secure cabling in data processing facilities. - ensuring equipment maintenance is contracted and performed in data processing facilities. <p>ISO 27001:2005 A.6.1.4, A.9.1.3, A.9.1.5, A.9.2.2, A.9.2.3, A.9.2.4</p>	
ITS2	Operational integrity and availability risk	A
	<p>Risk of loss of integrity or use of IT resources due to inadequate documentation, change management, or monitoring. Risk controls include:</p> <ul style="list-style-type: none"> - documenting operating procedures. - using formal change management to ensure stable operations. - separating development, test, and production environments. - maintaining and analyzing system event and log files. - protecting system log files. <p>ISO 27001:2005 A.10.1.1, A.10.1.2, A.10.1.4, A.10.10.1, A.10.10.2, A.10.10.3, A.10.10.6; SANS CC6</p>	
ITS3	Disaster risk	A
	<p>Risk of loss of use of IT resources due to a disruptive event. Disruptive events could include natural disasters, hackers, application errors, or user error. Risk controls include:</p> <ul style="list-style-type: none"> - creating backup copies of data. - storing backups in a secure, offsite location. - developing and testing a disaster recovery plan. <p>ISO 27001:2005 A.10.5.1, A.14.1.3; SANS CC19</p>	
ITS4	Network-related risk	A
	<p>Risk of attack of IT resources via the network due to inadequate network security or network flaws; risk of inability to use network or network services. Risk controls include:</p> <ul style="list-style-type: none"> - implementing a securely designed network. - implementing a securely designed wireless network. - implementing a securely designed network perimeter. - using secure network device configurations. - preventing unauthorized access to network services. <p>ISO 27001:2005 A.10.6.1, A.10.6.2, A.11.4.1, A.11.4.5, A.11.4.6, A.11.4.7; SANS CC4, CC5, CC13, CC14, CC16</p>	

ITS5	System-related risk	A
	Risk of attack of IT resources via the operating system due to inadequate system security or system flaws; risk of inability to use systems or application services. Risk controls include: <ul style="list-style-type: none"> - implementing securely configured systems. - maintaining a configuration management database. - implementing a operating system and application patch management system. - controlling the use of operating system and application privileges. 	
	ISO 27001:2005 A.11.2.2, A.12.4.1, A.12.5.2, A.12.6.1; SANS CC3, CC8	
ITS6	Identity-related risk	A
	Risk of unauthorized access or modification of information resources due to inadequate management of user accounts and passwords. Risk controls include: <ul style="list-style-type: none"> - assigning user accounts and passwords securely. - requiring secure logon to all systems and applications. - implementing good password management. - monitoring account usage. 	
	ISO 27001:2005 A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.1, A.11.5.3; SANS CC11	
ITS7	Malicious software risk	A
	Risk of unauthorized access or modification of information resources due to inadequate protection against malicious software attack; risk of inability to access of IT resources due to inadequate protection against malicious software attack. Risk controls include: <ul style="list-style-type: none"> - installing and maintaining anti-virus software on applicable devices. 	
	ISO 27001:2005 A.10.4.1; SANS CC12	
ITS8	Mobile worker-related risk	A
	Risk of unauthorized access or modification of information resources due to inadequate protection of mobile computing resources. Risk of theft of mobile devices. Includes laptop systems, PDAs, and smart-phones. Risk controls include: <ul style="list-style-type: none"> - maintaining an inventory of mobile devices. - providing appropriate security for mobile devices. - providing appropriate security for mobile workers using mobile devices in unprotected environments. - requiring strong authentication for remote access to information resources. 	
	ISO 27001:2005 A.9.2.5, A.9.2.7, A.11.4.2, A.11.7.1	

ITS9	Third party service management risk	B
	Risk of information assets being accidentally or maliciously compromised due to inadequate management and monitoring of third party providers. Limited to IT service providers. Risk controls include: <ul style="list-style-type: none"> - ensuring compliance with service level agreements (SLA's). - monitoring third party service providers. - verifying the information security provided by third parties. 	
	ISO 27001:2005 A.10.2.1, A.10.2.2, A.10.2.3	
ITS10	Message service-related risk	B
	Risk of unauthorized access to messages due to inadequately secured message system. Includes email, instant messaging, and any other messaging systems in use. Risk controls include: <ul style="list-style-type: none"> - protecting Email systems. - limiting unsolicited bulk Email (Spam). - protecting instant messaging and other messaging systems. 	
	ISO 27001:2005 A.10.8.4	
ITS11	Web/eCommerce-related risk	B
	Risk of unauthorized access or modification to information on web-based or eCommerce-based applications due to inadequate security. Risk controls include: <ul style="list-style-type: none"> - providing secure web or eCommerce services. - providing secure online transaction processing (OLTP) services. 	
	ISO 27001:2005 A.10.9.1, A.10.9.3	
ITS12	Security incident-related risk	B
	Risk of loss of use of IT resources due to inadequate response to and escalation of security incidents. Risk controls include: <ul style="list-style-type: none"> - using an incident handling procedure for managing events promptly. - reporting security weaknesses and vulnerabilities. 	
	ISO 27001:2005 A.13.1.1, A.13.1.2; SANS CC18	

ITS13	Storage media-related risk	B
	Risk of loss or exposure of confidential data due to inadequate management of storage media. Includes USB keys, memory cards, magnetic media, and optical media. Risk controls include: <ul style="list-style-type: none"> - managing the use of removable media or storage devices. - providing for the secure disposal of media - providing for the secure transportation of media 	
	ISO 27001:2005 A.10.7.1, A.10.7.2, A.10.8.3; SANS CC15	
ITS14	Service planning-related risk	C
	Risk of loss of use of IT resources due to inadequate capacity planning. Risk controls include: <ul style="list-style-type: none"> - ensuring the availability of future computing resources. - ensuring the availability of future infrastructure. 	
	ISO 27001:2005 A.10.3.1	