IBM Security Solutions for a Smarter Planet:

The IBM Security Framework and ISO 27002:2005

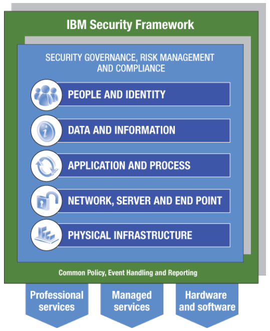
IBM Software

PCTY2010

Pulse Comes to You

Optimising the World's Infrastructure

27 May 2010 - London



IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

Discussion Topics:

- Introduction to Smarter Planet
- Supporting ISO 27002:2005 Best Practices
- IBM: Best Security Company

The Smarter Planet enables innovative change which inherently introduces new risks…

The planet is getting more…

Instrumented

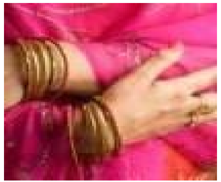
Interconnected

Intelligent

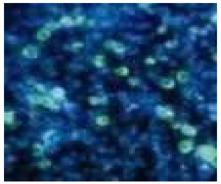
IBM helps you manage the security risks introduced by **Smarter Planet technology and business models** such as:

- Cloud computing and virtualization
- Federation with vendors and business partners
- Employee models – teleworking, outsourcing…

Smart supply chains


Smart countries

Smart retail


Smart water management

Smart weather

Smart energy grids

Intelligent oil field technologies

Smart regions

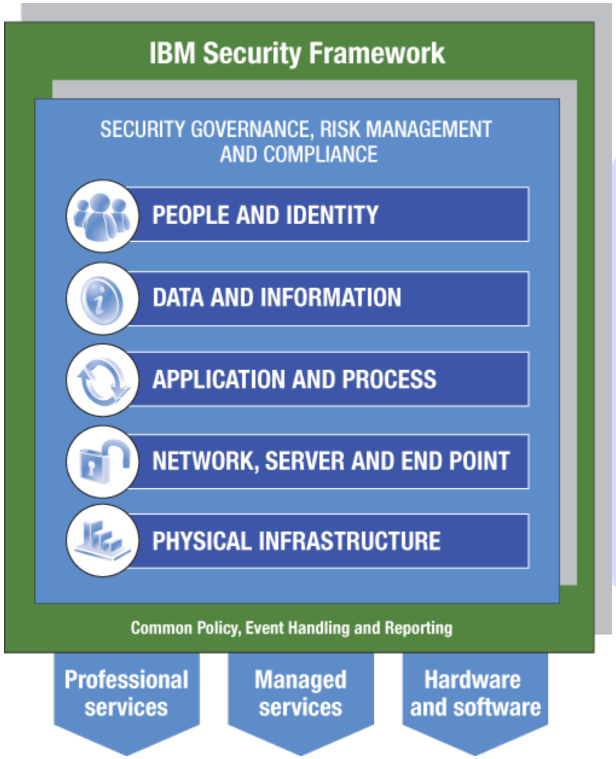
Smart healthcare

Smart traffic systems

Smart cities

Smart food systems

IBM Security Framework supports Integrated Service Management helping you assess and manage risk



GOVERANCE, RISK MGMT AND COMPLIANCE
Ensure comprehensive management of security activities and compliance with all security mandates

PEOPLE AND IDENTITY
Mitigate the risks associated with user access to corporate resources

DATA AND INFORMATION
Understand, deploy, and properly test controls for access to and usage of sensitive data

APPLICATION AND PROCESS
Keep applications secure, protected from malicious or fraudulent use, and hardened against failure

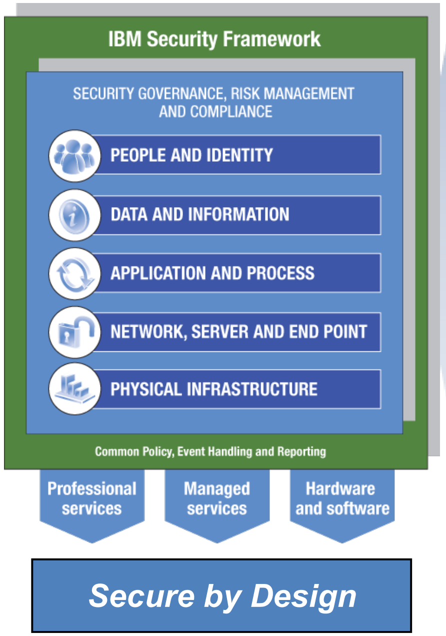
NETWORK, SERVER AND END POINT
Optimize service availability by mitigating risks to network components

PHYSICAL INFRASTRUCTURE
Provide actionable intelligence on the desired state of physical infrastructure security and make improvements

IBM Security Framework & Security Solutions Portfolio

🟩 = Services

🟪 = Products



IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

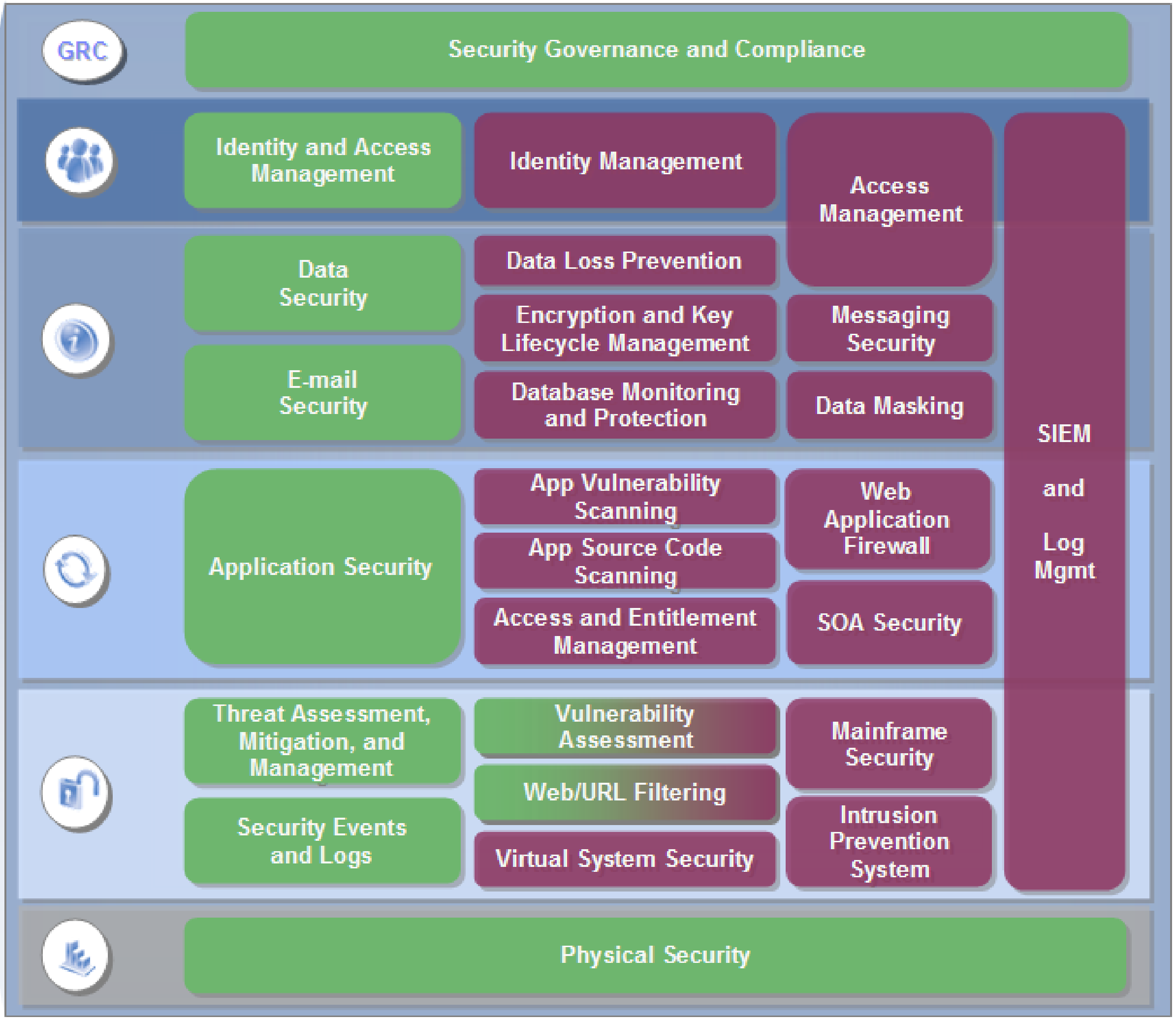
Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

Secure by Design



GRC

Security Governance and Compliance

Identity and Access Management

Identity Management

Access Management

Data Security

Data Loss Prevention

Encryption and Key Lifecycle Management

Messaging Security

E-mail Security

Database Monitoring and Protection

Data Masking

Application Security

App Vulnerability Scanning

App Source Code Scanning

Access and Entitlement Management

Web Application Firewall

SOA Security

Threat Assessment, Mitigation, and Management

Vulnerability Assessment

Web/URL Filtering

Mainframe Security

Security Events and Logs

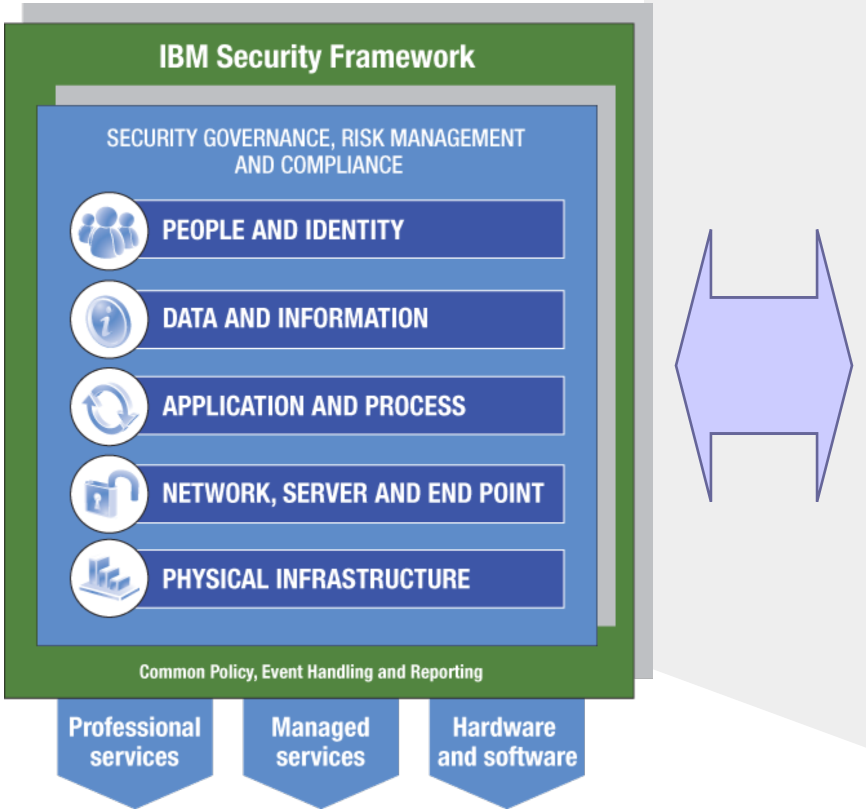
Virtual System Security

Intrusion Prevention System

SIEM and Log Mgmt

Physical Security

Comprehensive Support for ISO 27002 Security Controls is provided through the IBM Security Framework



- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Mgmt
- Access Control
- Information Systems Acquisition, Development a
- Information Security Incident Management
- Business Continuity Management
- Compliance

How we can help:

IBM understands
Security & Risk
are business problems first,
technical problems second

IBM has the
client success stories
to demonstrate results

IBM has deep
industry expertise

IBM has a huge
ecosystem of leading
security partners

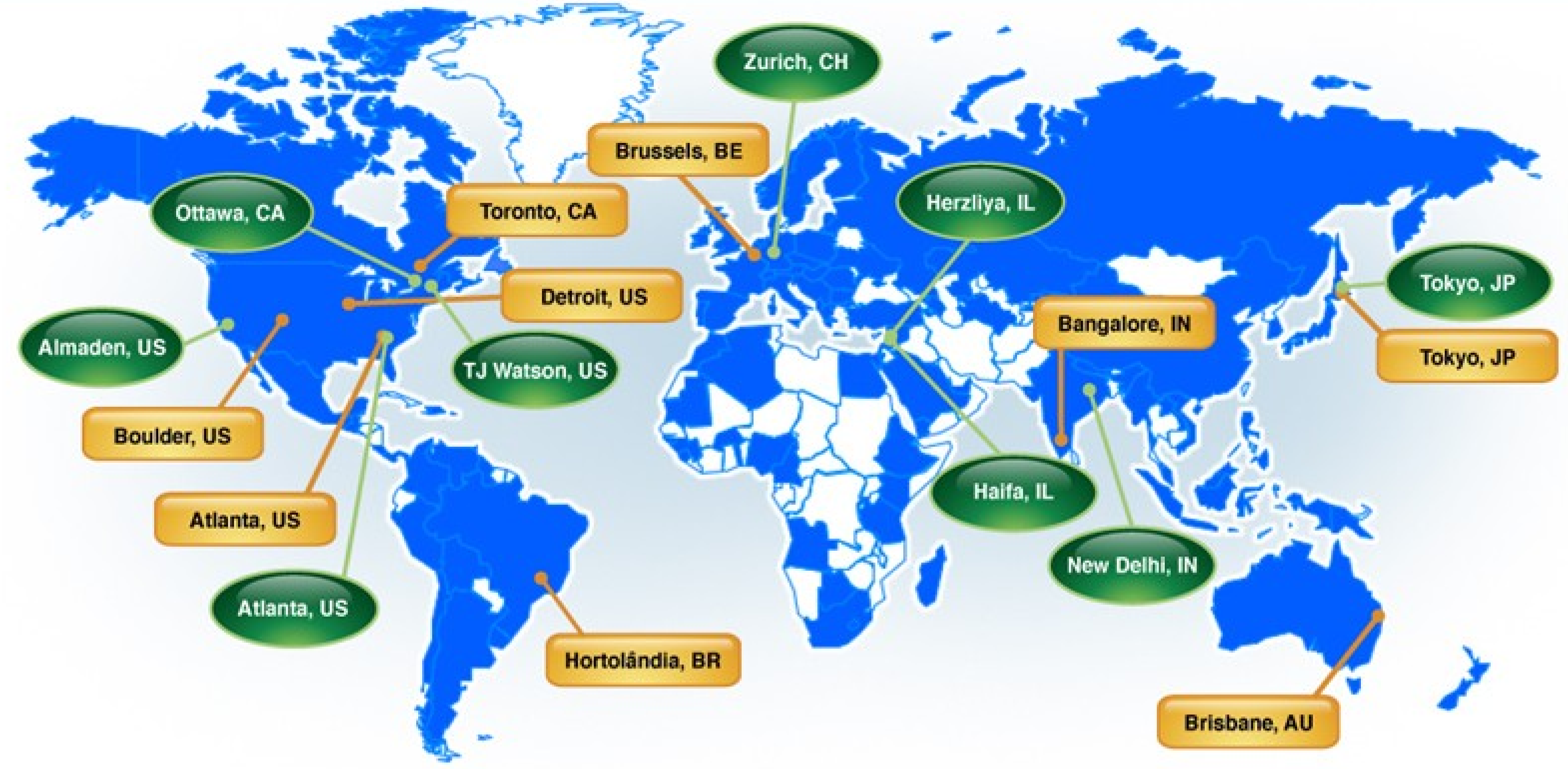
IBM has
industry's broadest
Security Solutions portfolio

IBM leverages our skills
to help meet your goals

Thank
You

Why IBM: Global Security Reach for IBM Security

9 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 30,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 8 Billion+ Events Per Day



ISO Support Details

Risk Assessment and Treatment

Capabilities	Benefits	IBM Offerings
Assessing and prioritizing security risks: •Identify, quantify risks •Recommend actions and implementation	Impartial risk management assessment with prioritized recommendations	IBM Security and Privacy Consulting Services
Treating Security Risks options: •Apply appropriate controls •Accept risks based on policy •Avoiding risks •Transferring risks to other parties	Optimize risk treatment plans to minimize risks and reduce exposures	

Security Policy

Capabilities	Benefits	IBM Offerings
Information Security Policy Document: Documentation, approval, publication, and communication	Establish security policy in accordance with business requirements, relevant laws and regulations	IBM Security & Privacy Consulting Services: Security Policy Definition Service
Information Security Policy Review: Periodic review for suitability, adequacy and effectiveness	Effective management of information security policy over time to ensure compliance and prevent new risks	IBM Security & Privacy Consulting Services: Security Healthcheck Service

Organization of Information Security

Capabilities	Benefits	IBM Offerings
Management commitment to information security and responsibilities	Establish commitment to manage information security to minimize risk	IBM Security & Privacy Consulting Services: Security Process Development Service
Information security activity co-ordination across organization	Establish responsibility and roles to achieve compliance and minimize risk	
Allocation of information security responsibilities	Ensure security policy responsibility for enforcement to minimize risks	IBM Security & Privacy Consulting Services: Enterprise Security Architecture Service
Authorization process for information processing facilities	Prevent unauthorized activities and comply with policy	
Confidentiality agreements – identity and review NDA and confidentiality	Protect the confidentiality of the information with outsiders	IBM Security & Privacy Consulting Services: Security Healthcheck Service
Contact with relevant authorities	Establish liaisons with authorities to manage risks	
Contact with special interest groups	Network with other security specialists to stay knowledgeable of risks	
Independent review of information security	Prevent security oversight and insider abuse	

Asset Management

Capabilities

Responsibility for assets:

- Inventory of important assets
- Ownership of assets
- Identity, document and implement acceptable use rules of assets

Information Classification:

- Classification guidelines based on value, legal requirements, sensitivity and criticality
- Information labeling and handling procedures based on classification

Benefits

Achieve and maintain protection of critical business assets to comply with security policy

Ensure that critical business assets are appropriately protected for compliance

IBM Offerings

IBM Security & Privacy Consulting Services - Information Asset Profile Service

IBM Security & Privacy Consulting Services – Security Process Development Service

IBM Security & Privacy Consulting Services – IBM Classification Module - Information Asset Profile Service

Tivoli Asset Management (Maximo, TADDM, TLCM)

Rational Asset Manager

Human Resources Security

Capabilities

Prior to employment:

•Define and document roles and responsibilities

•Background screening of employees, contractors and third party users

•Terms and conditions of employment with respect to information security

During Employment:

•Manage security requirements of users

•Information security awareness & educ

•Disciplinary process for security breach

Termination or change of employment:

•Termination responsibilities

•Return of assets

•Removal of asset rights

Benefits

Ensure that staff understands their responsibilities to reduce fraud, theft and misuse of resources

Ensure staff supports security policy to protect resources and reduce the risk of human error

Ensure that staff leaving the company do not to compromise security

IBM Offerings

IBM Security & Privacy Consulting Services – Security Policy Development Service

IBM Security & Privacy Consulting Services – Security Policy Development Service

IBM Identity & Access Mgmt Service

Tivoli Identity Manager integrated with HRMS, Role Mgmt Asst and Role Modeling Asst

IBM Identity & Access Mgmt Service

Single View of a Person – Entity Analytics

Tivoli Asset Management: Maximo

Physical and Environmental Security

Capabilities	Benefits	IBM Offerings
Secure areas: •Physical security perimeter •Physical entry controls •Secure Offices, rooms and facilities •Protect against external threats •Physical protection working secure areas •Public access, delivery and loading areas	Prevent unauthorized physical access, damage and interference with systems	IBM Security & Privacy Consulting Services, Site Security Assessment, IBM Digital Video Surveillance, TIM IBM Security & Privacy Consulting Services – Security Policy Development Service
Equipment security: •Equipment siting and protection •Supporting utilities backup •Power and telecomm cabling security •Equipment maintenance •Security of equipment off-premises •Secure disposal or re-use of equipment •Removal or property	Prevent loss, damage, theft or compromise of assets and interruption of business activities	IBM Business Continuity & Resilience Services Maximo – Tracking maintenance schedules

Communications and Operations Management

Capabilities

Operational procedures and responsibilities (change mgmt and Segregation of Duties):

Third party service delivery management

System planning and acceptance

Protection against malicious and mobile code

Back-up

Network security management

Media handling

Exchanges of information

Electronic commerce services

Monitoring

Benefits

Ensure secure operations and prevent internal abuse

Prevent third party security exposures and abuse

Minimize the risk of system failures and business disruptions

Maintain the integrity & availability of information and services

Protect information in networks and the supporting infrastructure

Prevent unauthorized disclosure, modification, removal or destruction of assets

Maintain the security of information and software across organizations

Ensure the security of electronic commerce services and their use

Detect unauthorized information processing activities

IBM Offerings

IBM Security & Privacy Consult Serv

IBM Security Event & Log Mgmt Serv

IBM Managed Security Services

IBM DLP services and partners

Tivoli Asset Management: Tivoli Configuration Mgr, TSRM, TCCMD

Tivoli Security Management: TIM, PIM, TFIM, TAMeb, TAMOS, TSIEM, TSPM, TKLM, zSecure Audit

Guardium, Optim Data Privacy Sol

IBM Virtual Security Server

Netcool Family - Netcool Performance Manager, ITCAM, ITM

Proventia IPS, AppScan, DataPower,

Tivoli Storage Management: TSM TCDP

Storage device encryption

Details

Summary List

Access Control

Capabilities

Business requirement for access control policy

User access management

User responsibilities

Network access control

Operating system access control

Application and information access control

Mobile Computing and teleworking

Benefits

Control access to information based on security policy

Ensure authorized access and protect information

Prevent unauthorized user access, compromise, or theft of information

Prevent unauthorized access to networked services based on security policy

Prevent unauthorized access to systems

Prevent unauthorized access to information held in application systems

Ensure information security when using mobile computing and teleworking facilities

IBM Offerings

IBM Security & Privacy Consulting Services – Secure Policy Development

IBM Identity and Access Mgmt Service

GTS Total Authentication Solution

Tivoli Security management: TIM, TFIM, TAMeb, TAMOS, TSPM, TAM ESSO, PIM, TDS, TSCM, TSIEM

Mainframe security: RACF, zSecure

Proventia Intrusion Prevention

Tivoli Asset Mgmt: Netcool, Maximo,

z/OS and AIX labeling and//or virtualization,

z/OS PKI Services

AIX and i5/os system,

IBM Virtual Server Security, LPARs, zVM

Lotus Mobile Connect

This slide intentionally left blank

Information Systems Acquisition, Development and Maintenance

Capabilities

Security requirements of Information Systems

Correct processing in applications

Cryptographic controls

Security of system files

Security in development and support processes

Technical Vulnerability Management

Benefits

Ensure security policy is an integral part of information systems lifecycle

Prevent errors, loss, unauthorized modification or misuse of information

Protect the confidentiality, authenticity, and integrity of information with cryptographic means

Ensure the security of system files to prevent business disruption

Maintain the security of application system software and information

Reduce risks resulting from exploitation of published technical vulnerabilities

IBM Offerings

IBM Security & Privacy Consulting Services

IBM Vulnerability Management Service

IBM Managed Security Services

IBM DLP Security Services

Tivoli Security Management: TSPM, TAMeb, TKLM, TAM, TSCM

Network Security: DataPower, Proventia

Asset Management: TSRM, TCCMD, TPM,

Data Security: Optim Data Privacy

Application Security: Rational Software Analyzer, Rational Clearcase & Team Concert, Rational AppScan, Rational Purify

Information Security Incident Management

Capabilities

Reporting information security events and weaknesses:

- Reporting information security events
- Reporting security weaknesses

Management of information security incidents and improvements:

- Responsibilities and procedures
- Learning from security incidents
- Collection of evidence

Benefits

Ensure information security events and weaknesses are communicated and handled quickly

Ensure a consistent and effective approach to manage security incidents

IBM Offerings

IBM Vulnerability Mgmt Service

IBM Security Event & Log Mgmt Service

IBM Security & Privacy Consulting Services

IBM Managed Security Services

Tivoli Security Management: TSIEM, TSCM

Mainframe Security: zSecure Audit

Proventia Site Protector

Application Security: Rational AppScan

Business Continuity Management

Capabilities

Aspects of business continuity management:

- Including information security in business continuity management process
- Business continuity and risk management
- Developing and implementing continuity plans including information security
- Business continuity planning framework
- Testing, maintaining and re-assessing business continuity plans

Benefits

Counteract interruptions to business activities and protect critical business processes from failures or disasters and ensure their timely resumption

Continuous availability of systems and information

IBM Offerings

IBM Business Continuity & Resiliency Services

Tivoli Storage Management

Compliance

Capabilities	Benefits	IBM Offerings
Compliance with legal requirements: •Identification of applicable legislation •Intellectual property rights •Protection of organizational records •Data protection and privacy •Prevention of misuse of IT facilities •Regulation of cryptographic controls	Avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements	IBM Security & Privacy Consulting Services IBM Identity & Access Mgmt Service IBM Vulnerability Management Service Tivoli Security Management: TKLM, TAMOS, TIM, TSM, TCDP,TSPM, TAMeb, TSIEM Mainframe security: RACF, zSecure Audit, Data Security: Guardium, Optim Data Privacy Application Security: Rational AppScan Storage devices with encryption capabilities
Compliance with policies & standards: • Compliance with policies and standards •Technical compliance checking	Ensure compliance of systems with organizational security policies and standards	
Information Systems audit : •Information systems audit controls •Protection of audit tools	Maximize the effectiveness and minimize interference to/from the information systems audit process	

12 ISO Security Control Sections - Descriptions

ISO 27002 Contents	Description
4. Risk Assessment and Treatment	To assess the current or potential security risks and determine the best method to address those risks.
5. Security Policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
6. Organization of Information Security	To manage and plan information security within the organization, taking into account the needs of both internal and external parties.
7. Asset Management	To deliver appropriate levels of protection and ensure that information receives a level of protection that is appropriate to its needs.
8. Human Resources Security	To ensure that staff, during employment, after termination and during change of employment, are part of the information security process.
9. Physical and Environmental Security	To secure buildings, locations and equipment in such a way as to prevent unauthorized physical access, damage and interference to the organization's assets, premises and information.
10. Communications and Operations Man	To ensure that information is treated properly, backed up correctly and handled securely to the highest standards available.
11. Access Control	To control access to information, networks, and applications. Preventing unauthorized access, interference, damage and theft.
12. Information Systems Acquisition, Dev	To ensure that security is an integral part of the information system. Securing applications, files and reducing vulnerabilities.
13. Information security incident manager	To ensure information security events and weaknesses are communicated consistently in a manner allowing timely corrective action to be taken.
14. Business Continuity Management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
15. Compliance	To avoid breaches of any law, regulation or contractual obligations. To ensure compliance without adverse affects on Information Security.

4. Risk Assessment and Treatment	IBM Support	Comments
4.1: Assessing Security Risks		
Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization.	IBM Security & Privacy Consulting Services	
The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.		
The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.		
4.2: Treating Security Risks		
For each of the risks identified following the risk assessment a risk treatment decision needs to be made.	IBM Security & Privacy Consulting Services	
Possible options for risk treatment include: a) applying appropriate controls to reduce the risks; b) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance; c) avoiding risks by not allowing actions that would cause the risks to occur; d) transferring the associated risks to other parties, e.g. insurers or suppliers.		

5. Security Policy	**IBM Support**	**Comments**
5.1: Information security policy		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. • Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.		
5.1.1: Information security policy document Control: An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	IBM Security & Privacy Consulting Services	Security Policy Definition Service
5.1.2: Review of the information security policy Control: The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	IBM Security & Privacy Consulting Services	Security Healthcheck Service

6. Organization of Information Security	IBM Support	Comments
6.1: Internal organization		
Objective: To manage information security within the organization. • A management framework should be established to initiate and control the implementation of information security within the organization. • Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization. • If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.		
6.1.1: Management commitment to information security Control: Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	IBM Security & Privacy Consulting Services	Security Process Development Service
6.1.2: Information security co-ordination Control: Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.	IBM Security & Privacy Consulting Services	Security Process Development Service
6.1.3: Allocation of information security responsibilities Control: All information security responsibilities should be clearly defined.	IBM Security & Privacy Consulting Services	Security Process Development Service
6.1.4: Authorization process for information processing facilities Control: A management authorization process for new information processing facilities should be defined and implemented.	IBM Security & Privacy Consulting Services	Enterprise Security Architecture Service
6.1.5: Confidentiality agreements Control: Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	IBM Security & Privacy Consulting Services	Security Process Development Service
6.1.6: Contact with authorities Control: Appropriate contacts with relevant authorities should be maintained.	IBM Security & Privacy Consulting Services	Security Process Development Service
6.1.7: Contact with special interest groups Control: Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	IBM Security & Privacy Consulting Services	Security Process Development Service
6.1.8: Independent review of information security Control: The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security	IBM Security & Privacy Consulting Services	Security Healthcheck Service

7. Asset Management	**IBM Support**	**Comments**
7.1: Responsibility for assets		
Objective: To achieve and maintain appropriate protection of organizational assets. • All assets should be accounted for and have a nominated owner. • Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.		
7.1.1: Inventory of assets	Maximo, TADDM, TLCM, Rational Asset Manager, IBM Security & Privacy Services	Information Asset Profile Service
Control: All assets should be clearly identified and an inventory of all important assets drawn up and maintained.		
7.1.2: Ownership of assets	Maximo, TADDM, TLCM, Rational Asset Manager, IBM Security & Privacy Services	Information Asset Profile Service
Control: All information and assets associated with information processing facilities should be owned2 by a designated part of the organization.		
7.1.3: Acceptable use of assets	IBM Security & Privacy Consulting Services, Rational Asset Manager, IBM Security & Privacy Services	Security Process Development Service
Control: Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.		
7.2: Information classification	**IBM Support**	**Comments**
Objective: To ensure that information receives an appropriate level of protection. • Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information. • Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.		
7.2.1: Classification guidelines	IBM Security & Privacy Consulting Services, IBM Classification Module	Information Asset Profile Service
Control: Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.		
7.2.2: Information labeling and handling	IBM Security & Privacy Consulting Services	Security Process Development Service
Control: An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.		

8. Human Resources Security	IBM Support	Comments
8.1: Prior to employment		
Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. • Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. • All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs. • Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.		
8.1.1: Roles and responsibilities	IBM Security & Privacy Consulting Services, TIM	Role Mgmt Asst and Role Modeling Asst, TIM Integrated with an HRMS system, Security Policy Development Service
Control: Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization’s information security policy.		
8.1.2: Screening	Single View of a Person, Entity Analytics, IBM Security & Privacy Services	Security Policy Development Service
Control: Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.		
8.1.3: Terms and conditions of employment	IBM Security & Privacy Consulting Services	Security Policy Development Service
Control: As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization’s responsibilities for information security.		

8.2: During employment	**IBM Support**	**Comments**
Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. • Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization. • An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third party users to minimize possible security risks. A formal disciplinary process for handling security breaches should be established.		
8.2.1: Management responsibilities	IBM Security & Privacy Consulting Services	Security Policy Development Service
Control: Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.		
8.2.2: Information security awareness, education, and training	IBM Security & Privacy Consulting Services	Not a formal offering but material exists to propose Security Awareness Development
Control: All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.		
8.2.3: Disciplinary process	IBM Security & Privacy Consulting Services	Security Policy Development Service
Control: There should be a formal disciplinary process for employees who have committed a security breach.		

8.3: Termination or change of employment	**IBM Support**	**Comments**
Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner. • Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed. • Change of responsibilities and employments within an organization should be managed as the termination of the respective responsibility or employment in line with this section, and any new employments should be managed as described in section 8.1.		
8.3.1: Termination responsibilities	IBM Security & Privacy Consulting Service, TIM, IBM Identity & Access Mgmt Service	TIM Integrated with HRMS system, Security Policy Development Service
Control: Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.		
8.3.2: Return of assets	IBM Security & Privacy Consulting Service, Maximo, TIM	TIM integrated with HRMS system, and with an Asset Management system to provide automated workflows to ensure assets are returned, Security Policy Development Service
Control: All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.		
8.3.3: Removal of access rights	TIM, IBM Security & Privacy Consulting Service	Security Policy Development Service
Control: The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.		

9. Physical and Environmental Security	IBM Support	Comments
9.1: Secure areas		
Objective: To prevent unauthorized physical access, damage, and interference to the organization’s premises and information. • Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. • The protection provided should be commensurate with the identified risks.		
9.1.1: Physical security perimeter	IBM Security & Privacy Consulting Services, IBM Digital Video Surveillance	Site Security Assessment Service
Control: Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.		
9.1.2: Physical entry controls	IBM Security & Privacy Consulting Services, IBM Digital Video Surveilance, TIM	Managing security badge access control accounts, Site Security Assessment Service
Control: Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.		
9.1.3: Securing offices, rooms and facilities	IBM Security & Privacy Consulting Services, IBM Digital Video Surveillance	Site Security Assessment Service
Control: Physical security for offices, rooms, and facilities should be designed and applied.		
9.1.4: Protecting against external and environmental threats	IBM Business Continuity & Resliance Services, IBM Security & Privacy Consulting Services	Site Security Assessment Service
Control: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.		
9.1.5: Working in secure areas	IBM Security & Privacy Consulting Services, IBM Digital Video Surveillance	Site Security Assessment Service
Control: Physical protection and guidelines for working in secure areas should be designed and applied.		
9.1.6: Public access, delivery, and loading areas	IBM Security & Privacy Consulting Services, IBM Digital Video Surveillance	Site Security Assessment Service
Control: Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.		

9.2: Equipment security	**IBM Support**	**Comments**
Objectives: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities. • Equipment should be protected from physical and environmental threats. • Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.		
9.2.1: Equipment siting and protection Control: Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	IBM Security & Privacy Consulting Services, IBM Digital Video Surveillance	Site Security Assessment Service
9.2.2: Supporting utilities Control: Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	IBM Business Continuity & Resliance Services, IBM Security & Privacy Consulting Services	Site Security Assessment Service
9.2.3: Cabling security Control: Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.	IBM Security & Privacy Consulting Services	Site Security Assessment Service
9.2.4: Equipment maintenance Control: Equipment should be correctly maintained to ensure its continued availability and integrity.	Maximo	Tracking maintenance schedules
9.2.5: Security of equipment off-premises Control: Security should be applied to off-site equipment taking into account the different risks of working outside the organization’s premises.	IBM Security & Privacy Consulting Services	Security Policy Development Service
9.2.6: Secure disposal or re-use of equipment Control: All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	IBM Security & Privacy Consulting Services, PGP & other 3rd party offerings	Security Policy Development Service
9.2.7: Removal of property Control: Equipment, information or software should not be taken off-site without prior authorization.	IBM Security & Privacy Consulting Services, Maximo	Security Policy Development Service

10. Communications and Operations Management	IBM Support	Comments
10.1: Operational procedures and responsibilities		
Objective: To ensure the correct and secure operation of information processing facilities. • Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures. • Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.		
10.1.1: Documented operating procedures	IBM Security & Privacy Consulting Services	
Control: Operating procedures should be documented, maintained, and made available to all users who need them.		
10.1.2: Change management	TSRM, TCCMD (CCMDB), TCM, TIM	
Control: Changes to information processing facilities and systems should be controlled.		
10.1.3: Segregation of duties	TIM, TSIEM, PIM, TSPM, IBM Identity & Access Mgmt Service	
Control: Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.		
10.1.4: Separation of development, test, and operational facilities	Optim Data Privacy Solution, Virtualization (LPAR, zVM), ISS Virtual Security Server	
Control: Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.		
10.2: Third party service delivery management	**IBM Support**	**Comments**
Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. • The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.		
10.2.1: Service delivery	IBM Security & Privacy Consulting Services, TFIM	
Control: It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.		
10.2.2: Monitoring and review of third party services	TSIEM	TSIEM can support the monitoring of third-party activity within the target environment. Violations of policy are recorded, and can be used to trigger security event and incident response mechanisms.
Control: The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.		
10.2.3: Managing changes to third party services	TSRM, TCCMD (CCMDB), TCM, TIM, TFIM	
Control: Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.		

10.3: System planning and acceptance	**IBM Support**	**Comments**
Objective: To minimize the risk of systems failures. • Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. • Projections of future capacity requirements should be made, to reduce the risk of system overload. • The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.		
10.3.1: Capacity management	Netcool Performance Manager, ITCAM	
Control: The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.		
10.3.2: System acceptance	IBM Security & Privacy Consulting Services, Tivoli Configuration Manager	
Control: Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.		
10.4: Protection against malicious and mobile code	**IBM Support**	**Comments**
Objective: To protect the integrity of software and information. • Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. • Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.		
10.4.1: Controls against malicious code	Proventia IPS, IBM Managed Security Services, AppScan, DataPower, TAMeb	
Control: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.		
10.4.2: Controls against mobile code	Proventia IPS, IBM Managed Security Services, AppScan, DataPower, TAMeb	
Control: Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.		

10.5: Back-Up	**IBM Support**	**Comments**
Objective: To maintain the integrity and availability of information and information processing facilities. • Routine procedures should be established to implement the agreed back-up policy and strategy (see also 14.1) for taking back-up copies of data and rehearsing their timely restoration.		
10.5.1: Information back-up Control: Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	TSM, TCDP, TKLM	TKLM for DS8000/DS5000 encrypting storage and TS1120 tapes
10.6: Network security management	**IBM Support**	**Comments**
Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure. • The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. • Additional controls may also be required to protect sensitive information passing over public networks.		
10.6.1: Network controls Control: Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	Proventia IPS, DataPower, Netcool family	
10.6.2: Security of network services Control: Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided inhouse or outsourced.	Proventia IPS, DataPower, Netcool family	
10.7: Media handling	**IBM Support**	**Comments**
Objectives: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. • Media should be controlled and physically protected. • Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.		
10.7.1: Management of removable media Control: There should be procedures in place for the management of removable media.	TSM, TKLM, IBM DLP services and partners	TotalStorage 3494, TS3100, TS3200, TS3500 Tape Library Systems
10.7.2: Disposal of media Control: Media should be disposed of securely and safely when no longer required, using formal procedures.	IBM Security & Privacy Consulting Services	
10.7.3: Information handling procedures Control: Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.	IBM Security & Privacy Consulting Services	
10.7.4: Security of system documentation Control: System documentation should be protected against unauthorized access.	IBM Security & Privacy Consulting Services	

10.8: Exchanges of information	IBM Support	Comments
Objective: To maintain the security of information and software exchanged within an organization and with any external entity. • Exchanges of information and software between organizations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation (see clause 15). • Procedures and standards should be established to protect information and physical media containing information in transit.		
10.8.1: Information exchange policies and procedures Control: Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	IBM Security & Privacy Consulting Services, TFIM, DataPower	There needs to be a business agreement for federation of identities between two enterprises.
10.8.2: Exchange agreements Control: Agreements should be established for the exchange of information and software between the organization and external parties.	IBM Security & Privacy Consulting Services, TFIM, DataPower	
10.8.3: Physical media in transit Control: Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	TotalStorage 3494, TS3100, TS3200, TS3500 Tape Library Systems, TSM, TKLM+encrypted media, IBM DLP services & partners	
10.8.4: Electronic messaging Controls: Information involved in electronic messaging should be appropriately protected.	DataPower, Lotus Notes, TAMeb, PGP	
10.8.5: Business information systems Controls: Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.	IBM Security & Privacy Consulting Services	
10.9: Electronic commerce services	**IBM Support**	**Comments**
Objective: To ensure the security of electronic commerce services, and their secure use. • The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, should be considered. The integrity and availability of information electronically published through publicly available systems should also be considered.		
10.9.1: Electronic commerce Control: Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	TAMeb, TFIM, DataPower, TSPM	
10.9.2: On-Line Transactions Control: Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	TAMeb, TFIM, DataPower, TSPM	
10.9.3: Publicly available information Control: The integrity of information being made available on a publicly available system should be	TAMeb, TFIM, DataPower, TSPM	

10.10: Monitoring	**IBM Support**	**Comments**
Objective: To detect unauthorized information processing activities. • Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. • An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities. • System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.		
10.10.1: Audit logging	TSIEM, zSecure Audit, Guardium, IBM Security Event & Log Management Service	
Control: Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.		
10.10.2: Monitoring system use	TSIEM, zSecure Audit, Guardium, IBM Security Event & Log Management Service	
Control: Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.		
10.10.3: Protection of log information	DR550/DR650 Data Retention Systems, DS8000, DS5000, TS1130, TSIEM, TAMOS, TIM, TKLM, IBM Security Event & Log Management Service	
Control: Logging facilities and log information should be protected against tampering and unauthorized access.		
10.10.4: Administrator and operator logs	TSIEM, zSecure Audit, Guardium, IBM Security Event & Log Management Service	
Control: System administrator and system operator activities should be logged.		
10.10.5: Fault logging	ITM, Netcool, TSIEM, zSecure Audit, Guardium, IBM Security Event & Log Management Service	
Controls: Faults should be logged, analyzed, and appropriate action taken.		
10.10.6: Clock synchronization	N/A	Typically included as a built-in OS service
Controls: The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.		

11. Access Control	IBM Support	Comments
11.1: Business requirement for access control		
Objective: To control access to information. • Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. • Access control rules should take account of policies for information dissemination and authorization.		
11.1.1: Access control policy Control: An access control policy should be established, documented, and reviewed based on business and security requirements for access.	IBM Security & Privacy Consulting Services	Security Policy Development Service
11.2: User access management	**IBM Support**	**Comments**
Objective: To ensure authorized user access and to prevent unauthorized access to information systems. • Formal procedures should be in place to control the allocation of access rights to information systems and services. • The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.		
11.2.1: User registration Control: There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	TIM, IBM Identity & Access Mgmt Service	
11.2.2: Privilege management Control: The allocation and use of privileges should be restricted and controlled.	TIM, TAMeb, TAMOS, TFIM, TSPM, IBM Identity & Access Mgmt Service	
11.2.3: User password management Control: The allocation of passwords should be controlled through a formal management process.	TIM, TAM-ESSO, PIM, TAMeb, TDS, RACF+zSecure, IBM Identity & Access Mgmt Service	
11.2.4: Review of user access rights Control: Management should review users' access rights at regular intervals using a formal process.	TIM, IBM Identity & Access Mgmt Service	

11.3: User responsibilities	**IBM Support**	**Comments**
Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities. • The co-operation of authorized users is essential for effective security. • Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. • A clear desk and clear screen policy should be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.		
11.3.1: Password use	TSCM, TIM, TAM-ESSO, TAMeb, PIM, RACF+zSecure, IBM Identity & Access Mgmt Service	
Control: Users should be required to follow good security practices in the selection and use of passwords.		
11.3.2: Unattended user equipment	TAM-ESSO, TSCM, IBM Identity & Access Mgmt Service	
Control: Users should ensure that unattended equipment has appropriate protection.		
11.3.3: Clear desk and clear screen policy	TAM-ESSO, TSCM, IBM Identity & Access Mgmt Service	
Control: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.		

11.4: Network access control	**IBM Support**	**Comments**
Objective: To prevent unauthorized access to networked services. • Access to both internal and external networked services should be controlled. • User access to networks and network services should not compromise the security of the network services by ensuring: a) appropriate interfaces are in place between the organization’s network and networks owned by other organizations, and public networks; b) appropriate authentication mechanisms are applied for users and equipment; c) control of user access to information services in enforced.		
11.4.1: Policy on use of network services	Proventia, TAMOS, TSIEM, RACF+zSecure	
Control: Users should only be provided with access to the services that they have been specifically authorized to use.		
11.4.2: User authentication for external connections	Total Authentication Solution, Lotus Mobile Connect, TAMeb, TAM ESSO, TFIM, PIM, RACF+zSecure, IBM Identity & Access Mgmt Service	
Control: Appropriate authentication methods should be used to control access by remote users.		
11.4.3: Equipment identification in networks	Netcool, Maximo	
Control: Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.		
11.4.4: Remote diagnostic and configuration port protection	TAMOS	
Control: Physical and logical access to diagnostic and configuration ports should be controlled.		
11.4.5: Segregation in networks	Proventia, z/OS and AIX with security labels and/or virtualization (e.g., LPARs, z/VM, third party commercial and open source offerings)	
Control: Groups of information services, users, and information systems should be segregated on networks.		
11.4.6: Network connection control	Proventia, Lotus Mobile Connect	
Control: For shared networks, especially those extending across the organization’s boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).		
11.4.7: Network routing control	Netcool	Management of networking equipment
Control: Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business		

11.5: Operating system access control	IBM Support	Comments
Objective: To prevent unauthorized access to operating systems. • Security facilities should be used to restrict access to operating systems to authorized users. The facilities should be capable of the following: a) authenticating authorized users, in accordance with a defined access control policy; b) recording successful and failed system authentication attempts; c) recording the use of special system privileges; d) issuing alarms when system security policies are breached; e) providing appropriate means for authentication; f) where appropriate, restricting the connection time of users.		
11.5.1: Secure log-on procedures	TAM-ESSO, TAMOS, TFIM, PIM, native OS security (e.g., RACF+zSecure, PKI Services), IBM Identity & Access Mgmt Service	
Control: Access to operating systems should be controlled by a secure log-on procedure.		
11.5.2: User identification and authentication	TIM, Total Authentication Solution, PIM, TAMESSO, TAMeb, TAMOS, TFIM, RACF+zSecure, z/OS PKI Services, IBM Identity & Access Mgmt Service	All IBM products support unique identifiers
Control: All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.		
11.5.3: Password management system	TIM, TAM-ESSO, PIM, TDS, RACF+zSecure, AIX, i5/OS, IBM Identity & Access Mgmt Service	
Control: Systems for managing passwords should be interactive and should ensure quality passwords.		
11.5.4: Use of system utilities	TAMOS, RACF+zSecure, AIX, i5/OS	
Control: The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.		
11.5.5: Session time-out	TAMESSO, TSCM	
Control: Inactive sessions should shut down after a defined period of inactivity.		
11.5.6: Limitation of connection time	TAMeb, PIM	
Control: Restrictions on connection times should be used to provide additional security for high-risk applications.		

11.6: Application and information access control	**IBM Support**	**Comments**
Objective: To prevent unauthorized access to information held in application systems. • Security facilities should be used to restrict access to and within application systems. • Logical access to application software and information should be restricted to authorized users. Application systems should: a) control user access to information and application system functions, in accordance with a defined access control policy; b) provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls; c) not compromise other systems with which information resources are shared.		
11.6.1: Information access restriction Control: Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.	TAMeb, TAMOS, TSPM, TAMESSO, TFIM, PIM, TIM, TSCM, RACF+zSecure, AIX, i5/OS, IBM Identity & Access Mgmt Service	
11.6.2: Sensitive system isolation Control: Sensitive systems should have a dedicated (isolated) computing environment.	ISS Virtual Server Security, LPARs, zVM	Virtualization, operating systems with security label support for MLS, operating systems with SLS and secure guards
11.7: Mobile computing and teleworking	**IBM Support**	**Comments**
Objective: To ensure information security when using mobile computing and teleworking facilities. • The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.		
11.7.1: Mobile computing and communications Control: A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	IBM Security & Privacy Consulting Services, Lotus Mobile Connect, TSCM, TAMESSO	Security Policy Development Service
11.7.2: Teleworking Control: A policy, operational plans and procedures should be developed and implemented for teleworking activities.	IBM Security & Privacy Consulting Services, Lotus Mobile Connect	Security Policy Development Service

12. Information Systems Acquisition, Development and Maintenance	IBM Support	Comments
12.1: Security requirements of information systems		
Objective: To ensure that security is an integral part of information systems. • Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems. • All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.		
12.1.1: Security requirements analysis and specification	IBM Security & Privacy Consulting Services, TSRM, Rational family	
Control: Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.		
12.2: Correct processing in applications	**IBM Support**	**Comments**
Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications. • Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data. • Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.		
12.2.1: Input data validation	AppScan, Rational Software Analyzer, Rational Purify, DataPower, Proventia, IBM Managed Security Services	
Control: Data input to applications should be validated to ensure that this data is correct and appropriate.		
12.2.2: Control of internal processing	AppScan, Rational Software Analyzer, Rational Purify, DataPower, Proventia, IBM Managed Security Services	
Control: Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.		
12.2.3: Message integrity	DataPower, TSPM, TAMebRational Software Analyzer, Rational Purify, AppScan	
Control: Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.		
12.2.4: Output data validation	AppScan, Rational Software Analyzer, Rational Purify, DataPower, Proventia, IBM	
Control: Data output from an application should be validated to ensure that the processing of stored		

12.3: Cryptographic controls	**IBM Support**	**Comments**
Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means. • A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.		
12.3.1: Policy on the use of cryptographic controls	IBM Security & Privacy Consulting Services, TKLM, DataPower, TAMeb	
Control: A policy on the use of cryptographic controls for protection of information should be developed and implemented.		
12.3.2: Key management	TKLM	
Control: Key management should be in place to support the organization's use of cryptographic techniques.		
12.4: Security of system files	**IBM Support**	**Comments**
Objective: To ensure the security of system files. • Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.		
12.4.1: Control of operational software	TSRM, TCCMD (CCMDB), TPM, TSCM	
Control: There should be procedures in place to control the installation of software on operational systems.		
12.4.2: Protection of system test data	Optim Data Privacy	
Control: Test data should be selected carefully, and protected and controlled.		
12.4.3: Access control to program source code	Rational Clearcase & Team Concert	
Control: Access to program source code should be restricted.		

12.5: Security in development and support processes	IBM Support	Comments
Objective: To maintain the security of application system software and information. • Project and support environments should be strictly controlled. • Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.		
12.5.1: Change control procedures	TSRM, Rational Clearcase & Team Concert	12.5.1 to 12.5.5 refer to security controls during development and support processes. IBM products are Evaluation Assurance Level certified (common criteria). EAL certification addresses all of these requirements.
Control: The implementation of changes should be controlled by the use of formal change control procedures.		
12.5.2: Technical review of applications after operating system changes	AppScan	
Control: When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.		
12.5.3: Restrictions on changes to software packages	Rational Clearcase & Team Concert, TSRM	
Control: Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.		
12.5.4: Information leakage	IBM DLP Security Services	Partner products
Control: Opportunities for information leakage should be prevented.		
12.5.5: Outsourced software development	IBM Security & Privacy Consulting Services, AppScan	Security Policy Development Service
Control: Outsourced software development should be supervised and monitored by the organization.		

12.6: Technical Vulnerability Management	IBM Support	Comments
Objective: To reduce risks resulting from exploitation of published technical vulnerabilities. • Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.		
12.6.1: Control of technical vulnerabilities	IBM Vulnerability Management Service	
Control: Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate		

13. Information security incident management	IBM Support	Comments
13.1: Reporting information security events and weaknesses		
Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. • Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.		
13.1.1: Reporting information security events	TSIEM, TSCM, zSecure Audit, IBM Managed Security Services, Proventia SiteProtector, IBM Vulneraiblity Management Service, IBM Security Event & Log Management Service	
Control: Information security events should be reported through appropriate management channels as quickly as possible.		
13.1.2: Reporting security weaknesses	AppScan, TSIEM, TSCM, zSecure Audit, IBM Managed Security Services, IBM Vulnerability Management Service	
Control: All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.		
13.2: Management of information security incidents and improvements	**IBM Support**	**Comments**
Objective: To ensure a consistent and effective approach is applied to the management of information security incidents. • Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. • Where evidence is required, it should be collected to ensure compliance with legal requirements.		
13.2.1: Responsibilities and procedures	IBM Security & Privacy Consulting Services	Security Policy Development Service
Control: Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.		
13.2.2: Learning from information security incidents	TSIEM, zSecure Audit	
Control: There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.		
13.2.3: Collection of evidence	TSIEM, zSecure Audit, TSCM, Proventia SiteProtector, IBM Security Services, IBM Security Event & Log Management Service	
Control: Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).		

14. Business Continuity Management	IBM Support	Comments
14.1: Aspects of business continuity management		
Objective: Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. • A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.		
• The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization.		
• Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.		
14.1.1: Including information security in the business continuity management process	IBM Business Continuity & Resiliency Services, TSM	
Control: A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.		
14.1.2: Business continuity and risk assessment	IBM Business Continuity & Resiliency Services	
Control: Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.		
14.1.3: Developing and implementing continuity plans including information security	IBM Business Continuity & Resiliency Services, TSM	
Control: Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.		
14.1.4: Business continuity planning framework	IBM Business Continuity & Resiliency Services	
Control: A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.		
14.1.5: Testing, maintaining and re-assessing business continuity plans	IBM Business Continuity & Resiliency Services	
Control: Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.		

15. Compliance	IBM Support	Comments
15.1: Compliance with legal requirements		
Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. • The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. • Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).		
15.1.1: Identification of applicable legislation	IBM Security & Privacy Consulting Services	Security Policy Development Service - mostly focused on identifying legal counsel for the organization (IBM does not provide legal advice)
Control: All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.		
15.1.2: Intellectual property rights (IPR)	IBM Security & Privacy Consulting Services	Security Policy Development Service - mostly focused on identifying legal counsel for the organization (IBM does not provide legal advice)
Control: Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.		
15.1.3: Protection of organizational records	DR550/DR650 Data Retention Systems, TotalStorage Tape Library Systems, DS8000/DS5000 Encrypting Storage Systems w/ TKLM for key management, TAMOS, TIM, TSM, TCDP, TSIEM, Guardium, RACF+zSecure	Security Policy Development Service - mostly focused on identifying legal counsel for the organization (IBM does not provide legal advice)
Control: Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.		
15.1.4: Data protection and privacy of personal information	DR550/DR650 Data Retention Systems, TotalStorage Tape Library Systems, DS8000/DS5000 Encrypting Storage Systems w/ TKLM for key managementTSPM, TAMeb, TIM, TSIEM, Optim Data Privacy, RACF+zSecure, Guardium, AppScan, IBM Identity & Access Mgmt Service	Security Policy Development Service - mostly focused on identifying legal counsel for the organization (IBM does not provide legal advice)
Control: Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.		
15.1.5: Prevention of misuse of information processing facilities	TSIEM, zSecure Audit, Guardium, IBM Security & Privacy Consulting Services, IBM Identity & Access Mgmt Service	Security Policy Development Service
Control: Users should be deterred from using information processing facilities for unauthorized purposes.		
15.1.6: Regulation of cryptographic controls	IBM Security & Privacy Consulting Services, TKLM	Security Policy Development Service - mostly focused on identifying legal counsel for the organization (IBM does not provide legal advice)
Control: Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.		

15.2: Compliance with security policies and standards, and technical compliance	IBM Support	Comments
Objective: To ensure compliance of systems with organizational security policies and standards. • The security of information systems should be regularly reviewed. • Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.		
15.2.1: Compliance with security policies and standards	IBM Security & Privacy Consultilng Services	Security Policy Development Service
Control: Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.		
15.2.2: Technical compliance checking	TSIEM, zSecure Audit, Guardium, Rational AppScan, IBM Security & Priavacy Consulting Services, IBM Vulnerability Management Service	
Control: Information systems should be regularly checked for compliance with security implementation standards.		

15.3: Information systems audit considerations	IBM Support	Comments
Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process. • There should be controls to safeguard operational systems and audit tools during information systems audits. • Protection is also required to safeguard the integrity and prevent misuse of audit tools.		
15.3.1: Information systems audit controls	IBM Security & Privacy Consulting Services, TSIEM, zSecure Audit, Guardium, IBM Vulnerability Management Service	Security Policy Development Service
Control: Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.		
15.3.2: Protection of information systems audit tools	TSIEM, zSecure Audit, Guardium, DS8000, DS5000, TS1130	IBM tools have access control mechanisms built-in to prevent unauthorized access.
Control: Access to information systems audit tools should be protected to prevent any possible misuse or compromise.		

Summary of ISO Compliance Offerings and Business Benefits

Benefits	Why IBM	IBM Offerings
Address ISO and other compliance requirements with effective security policy assessment, recommendations and implementation Reduce complexity with automation and simplified controls Reduce costs with effective controls and automation Comprehensive family of security products, consulting services and managed security services Integrate security with HR, asset management, physical security and business recovery	Trusted long term security partner Comprehensive end-to-end security solutions Experienced global worldwide service capabilities Industry leading technology, products and research Industry specific knowledge and skills: utilities, healthcare, retail, financial, government, and more Extensive partner ecosystem Customer success stories and references	IBM Security & Privacy Consulting Services IBM Business Continuity & Resilience Services Tivoli Identity Manager family (TIM, TDS, PIM, Role Mgmt Asst and Role Modeling Asst, integration with RMS) Tivoli Access Manager family (TAMeb, TAMOS, TAM ESSO, TSPM, TFIM) Tivoli Security Information and Event Manager, Tivoli Key Lifecycle Manager, Tivoli Security Compliance Manager Tivoli Asset Management family (Maximo, TADDM, TLCM, TSRM, TCCMD, TCM, Netcool) System z: RACF and zSecure Audit Rational Asset Manager. AppScan Guardium, Optim Data Privacy Solution, Entity Analytics Proventia Intrusion Prevention System and Virtual Security Server