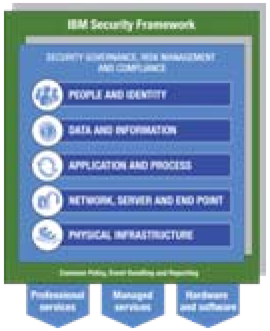
Security Solutions for a Smarter Planet:

IBM Directions in Security, Risk Management & Compliance

© 2010 IBM Corporation



Discussion Topics:

- Security on a Smarter Planet
- Introduction to the IBM Security Framework
- Supporting industry standard best practices for security
- Pulse ANZ Security Sessions

Welcome to the smarter planet

The planet is getting more

Instrumented, **Interconnected** and **Intelligent**.

Globalization and Globally Available Resources
Access to streams of information in the Realtime
INTERNET
facebook
myspace
iTunes
Google
Billions of mobile devices accessing the Web
New Forms of Collaboration

162 million

Almost 162 million smart phones were sold in 2008, surpassing laptop sales for the first time.

90%

Nearly 90% of innovation in automobiles is related to software and electronics systems.

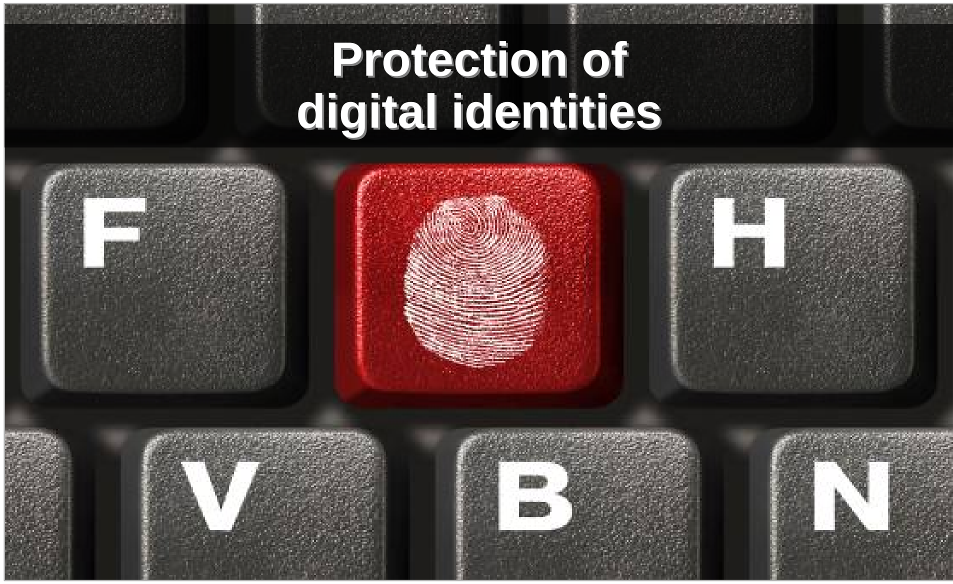
1 trillion

Soon, there will be 1 trillion connected devices in the world, constituting an “internet of things.”

With the smarter planet opportunities come **new security and privacy risks**

Protection of sensitive and large volumes of data, shared globally

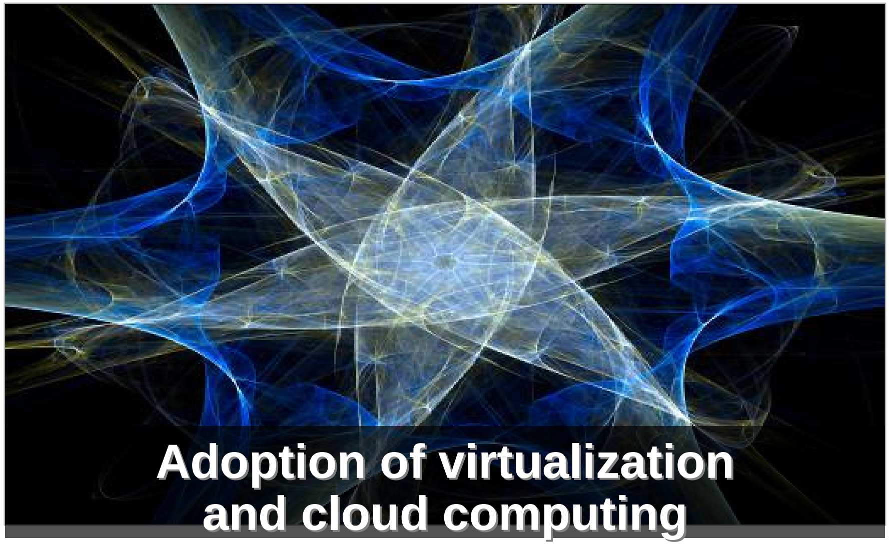
Protection of sensors and actuators in the wild



Protection of digital identities

Additional security and privacy risks impacting customers

Addressing the new cyber threat landscape



Adoption of virtualization and cloud computing

Addressing compliance complexity

Expectation of privacy

So how can security help us take advantage of opportunities on the smarter planet?

Security enables us to **take risks** and **innovate confidently**.

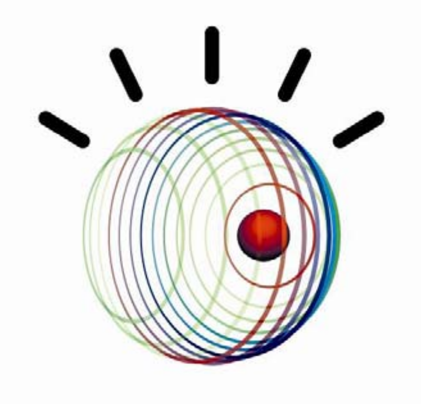
- Enables safe adoption of **new forms of technology** like cloud computing and virtualization
- Enables **new business models** like outsourcing and teleworking
- Addresses **emerging compliance constructs**, while decreasing IT operations costs
- Assures the quality, availability and integrity of information required for **real time decision making**
- Addresses **consumer expectation of privacy** by assuring "trusted brand" status

“Secure by design”

A new model for building a smarter planet

- **Security cannot solely be the job of regulators** or a stand-alone corporate department
- In an interdependent world, **security has become both a necessity and a collective responsibility** – one that we must take on as an intentional plan, not as an afterthought.
- We need to build solutions where **security is factored into the initial design** and is intrinsic to the business processes, product development lifecycle and daily operations.
  - Securely and safely adopt new technology and business models
  - Increase innovation and shorten time to market
  - Reduce security costs

…IBM can help



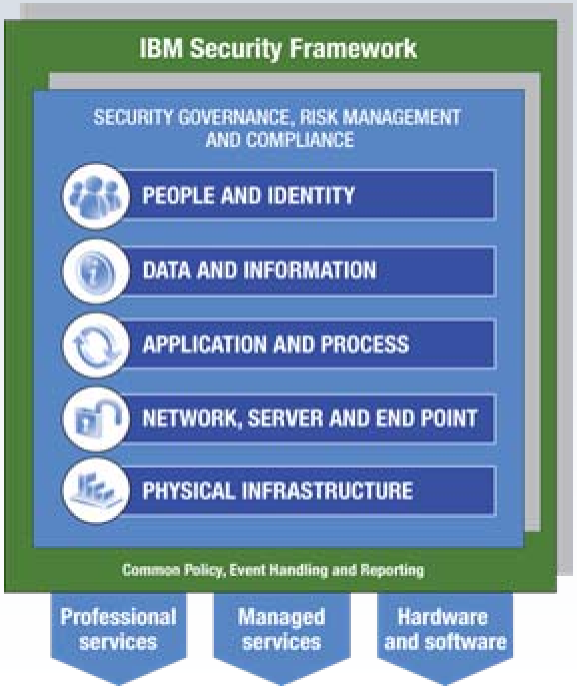
IBM’s security strategy

IBM Security Solutions. Secure by Design.

Delivering secure products and services

- **15,000** researchers, developers and SMEs on security initiatives
  - Data Security Steering Committee
  - Security Architecture Board
  - Secure Engineering Framework
- **3,000+** security & risk management patents
- Implemented **1000s** of security projects
- **40+** years of proven success securing the zSeries environment
- Managing **over 7 Billion** security events per day for clients
- **200+** security customer references and more than 50 published case studies

Providing end-to-end coverage across all security domains



So where do we start?
…… *many scenarios to plan for…*

External Threats

- Power failures

- Natural disasters
- Economic upheaval

- Malware
- Denial of service
- Sophisticated, organized attacks

Inadvertent

- Unpatched systems
- Code and application vulnerabilities
- Lack of change control
- Human error or carelessness

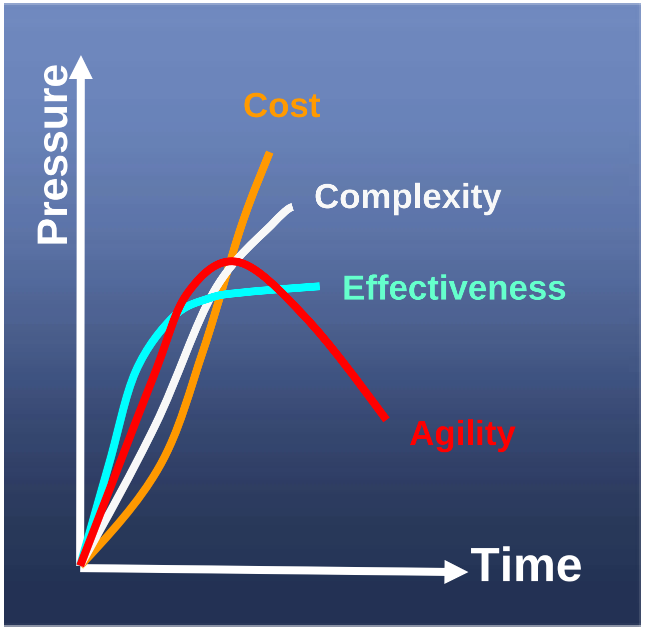
- Developer-created back door
- Information theft
- Insider fraud

Deliberate

Insider Threats

“Foundational Controls” = seatbelts and airbags

- **Find a balance between effective security and cost**
  - The axiom… never spend $100 dollars on a fence to protect a $10 horse
- **Studies show the Pareto Principle (the 80-20 rule) applies to IT security***
  - 87% of breaches were considered avoidable through reasonable controls
- **Small set of security controls provide a disproportionately high amount of coverage**
  - Critical controls address risk at every layer of the enterprise
  - Organizations that use security controls have significantly higher performance*
- **Focus on building security into the fabric of the business**
  - “Bolt on” approaches after the fact are less effective and more expensive
  - Use the small set of security controls as a starting point when designing a system



*Sources: W.H. Baker, C.D. Hylender, J.A. Valentine, 2008 Data Breach Investigations Report, Verizon Business, June 2008
ITPI: IT Process Institute, EMA December 2008

“Foundational Controls” represent a hygienic process…

- “From the attacker’s perspective, the rationale is simple: When foundational controls fail or do not exist, why seek a more challenging target? **Neglecting the fundamentals makes an organization an easy—and hence preferred—target.**” (EMA, 2009)
- Controls provide a solid foundation for IT Security Management
  - Identity and Access Management
  - Data and Information Protection
  - Release Management
  - Change and Configuration Management
  - Threat and Vulnerability Management
  - Problem and Incident Management
  - Security Information and Event Management
- High performers adhere to “Plan–Do–Check–Act” philosophy

Adherence to ITIL (ITSM) sets apart highest performers in security management

Visibility

Understand health and performance of services across your infrastructure

Control

Govern and secure complex infrastructure and ensure regulatory compliance

Automation

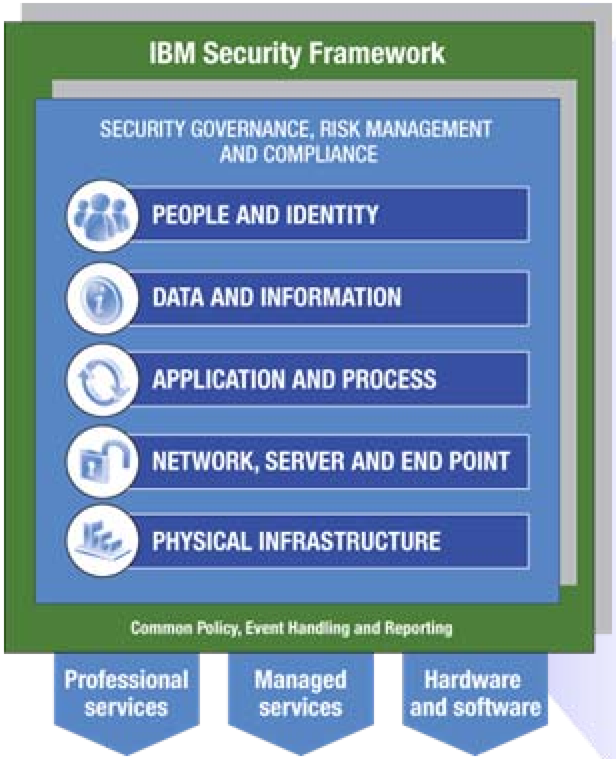
Drive down cost, minimize human error and increase productivity

…And “Foundational Controls” provide an effective approach for dealing with the growing compliance landscape

	Identity & Access Mgmt.	Data & Info Protection	Release Mgmt.	Change & Config Mgmt.	Threat & Vulnerability Mgmt.	Problem & Incident Mgmt.	Security Info & Event Mgmt.
Global Regulations							
SOX 404 & Variants	✓	✓	×	×	✓	✓	×
ISO27001	✓	✓	×	✓	✓	✓	✓
CobiT v4.1	✓	✓	✓	✓	✓	✓	✓
ITIL	×	×	✓	✓	×	×	×
PCI	✓	✓	×	✓	✓	✓	✓
Country / Regional Regulations							
Basel II	×	✓	×	×	✓	×	×
GLB	✓	✓	×	✓	✓	✓	✓
BITS	✓	✓	×	✓	×	×	✓
FFIEC	✓	✓	✓	✓	✓	✓	✓
EUDPD & member states data privacy directives	✓	✓	×	×	×	×	✓
PIPEDA	✓	✓	×	×	×	×	✓
NERC	✓	✓	✓	✓	✓	✓	✓
HIPAA	✓	✓	×	✓	✓	✓	✓
FISMA	×	×	×	✓	✓	✓	×

- Organizations face a growing number and complexity of compliance initiatives, many of which are evolving
- Foundational controls directly affect an organization’s information security posture.
- Prevalent compliance initiatives contain additional domains and control sets that fall under IT Management
  - For e.g., data backup/recovery processes, physical facility security, etc. affect an organization’s compliance posture, but are not considered foundational in terms of Information Security.

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



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

GRC

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

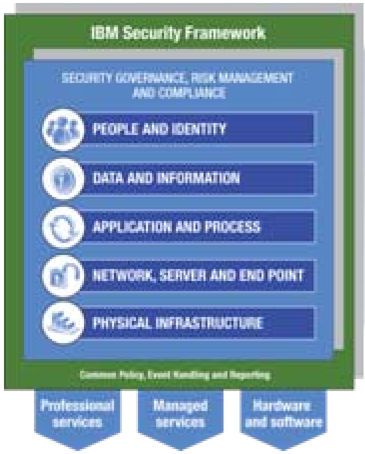
Provide actionable intelligence on the desired state of physical infrastructure security and make improvements

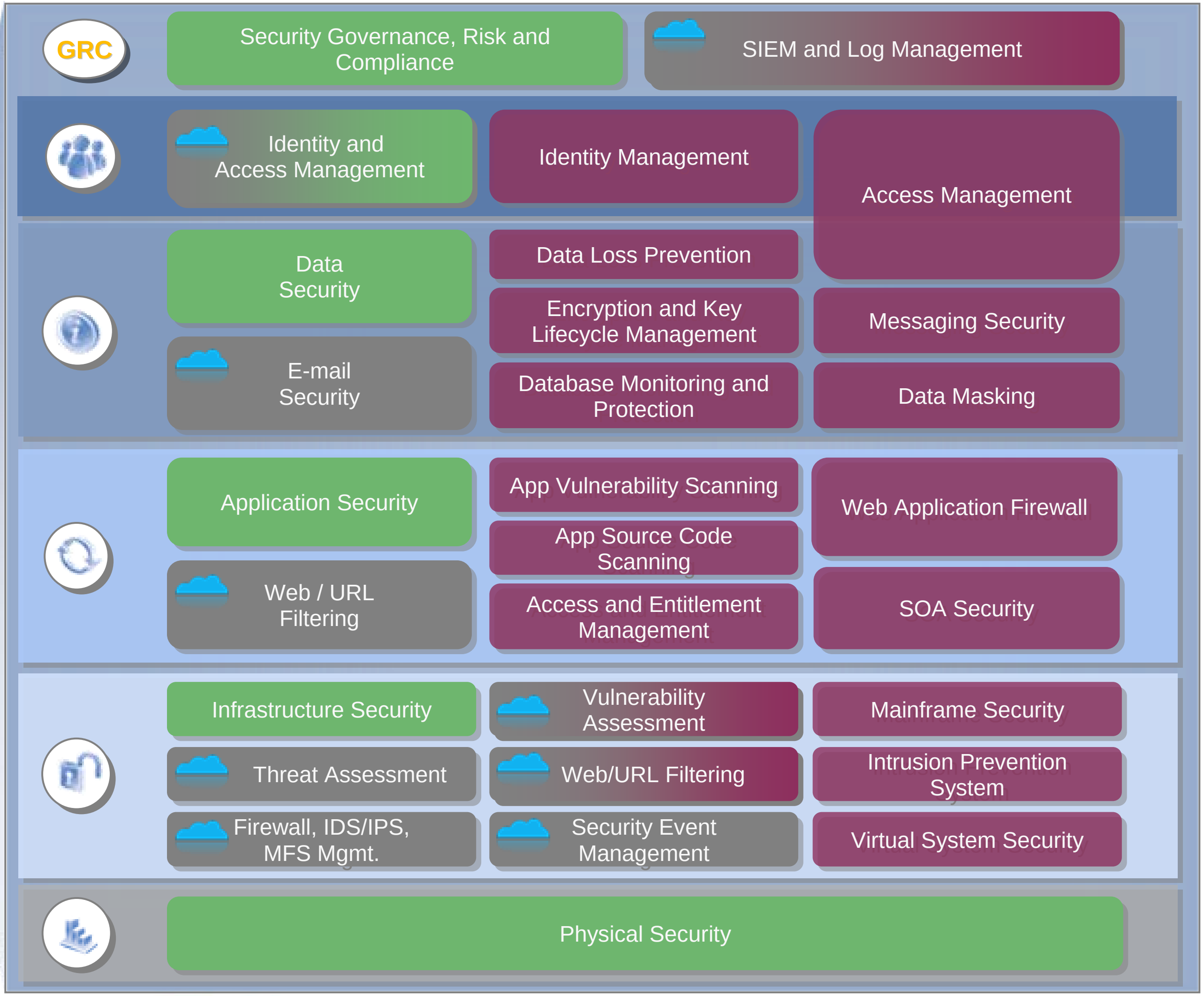
IBM security portfolio Overview

🟩 = Professional Services

☁ = Cloud-based & Managed Services

🟪 = Products





GRC

Security Governance, Risk and Compliance

☁ SIEM and Log Management

☁ 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

Web Application Firewall

App Source Code Scanning

☁ Web / URL Filtering

Access and Entitlement Management

SOA Security

Infrastructure Security

☁ Vulnerability Assessment

Mainframe Security

☁ Threat Assessment

☁ Web/URL Filtering

Intrusion Prevention System

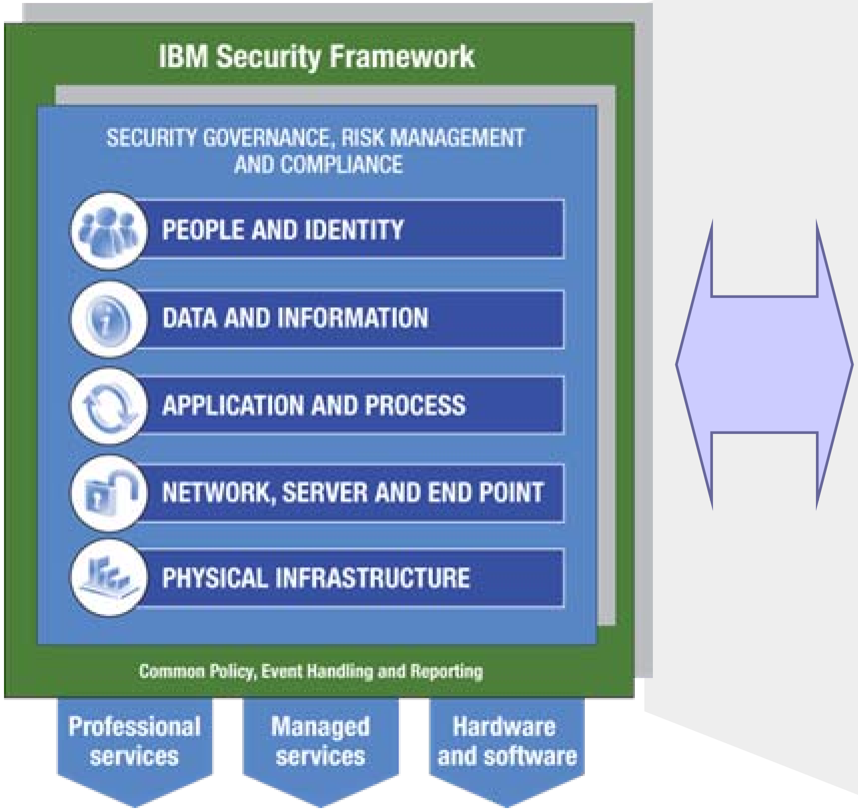
☁ Firewall, IDS/IPS, MFS Mgmt.

☁ Security Event Management

Virtual System Security

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 and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Example: 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

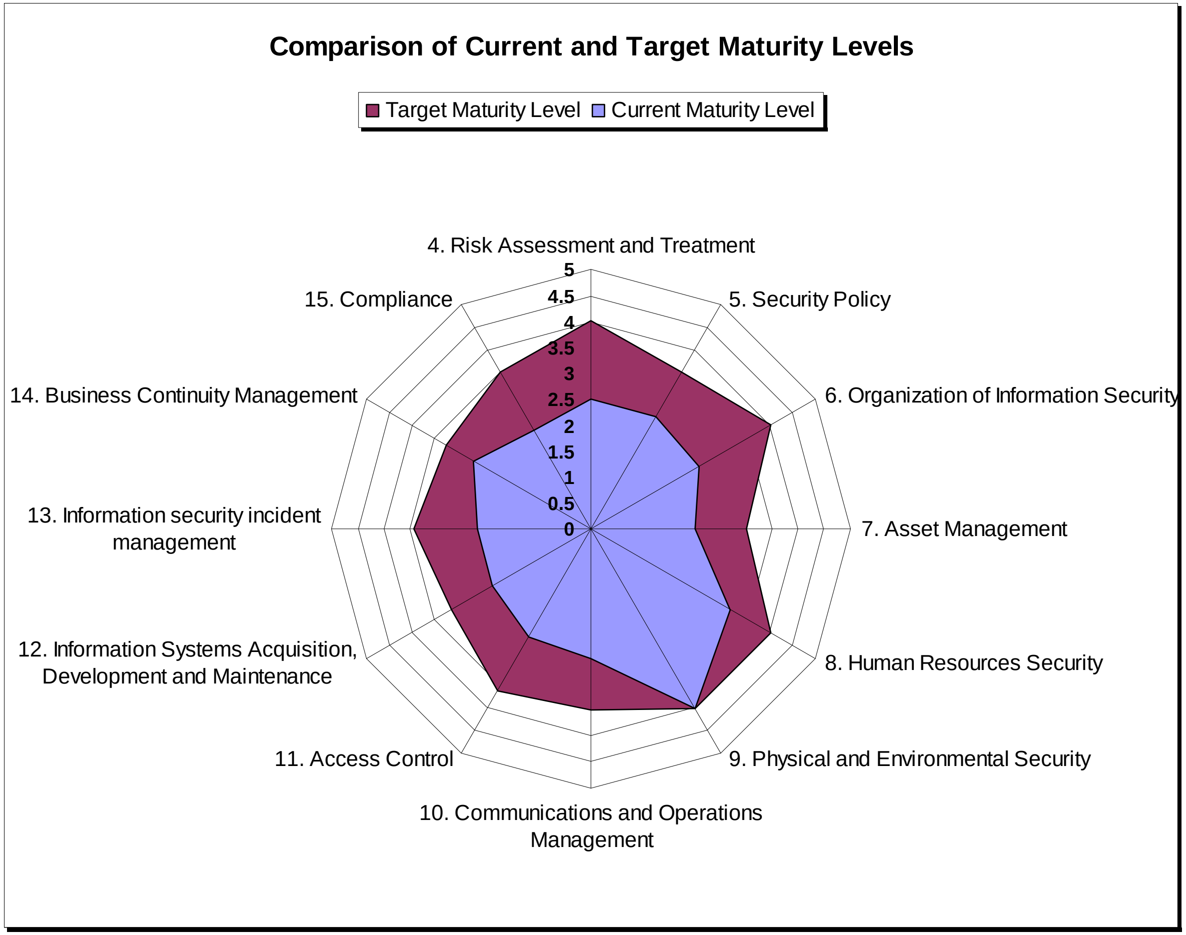
Proventia IPS, AppScan, DataPower,

Tivoli Storage Management: TSM TCDP

Storage device encryption

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.		

One way we can help: Facilitated ISO 27002 Gap Analysis for Your Organization



How we add value:

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

Security Track Day 1:

- Security Reference Architecture: a statement in Time to Value, James Darwin, WW Tivoli Security Solution Architect
- Audit and Compliance Best Practices: A practical guide to winning the war, Pete Stevenson, Manager, Tivoli Advanced Technology Group, SWAT Security Team
- A Solution Pattern for Multi-context Identity and Access Management, Neil Readshaw, IBM Australia Development Laboratory, Russell McClimont, Manager Information Security, IAG
- The Unprecedented State of Web Insecurity, Craig Lawson, Senior Security Consultant, IBM Australia

Security Track Day 2:

- Securing Virtualised Environments, Craig Lawson, Senior Security Consultant, IBM Australia
- The State of Database Compliance, Scott Henley, Consulting Security Specialist, IBM
- Who Said IT Security Was Boring? Garry Bentlin, Global Security Manager, IBM Certified Ethical Hacker, IBM Australia:
- Distributed ITIM (DTIM): A Solution for Large Scale Identity Mgt, Karthik Satishkumar, Tivoli Security Principal, IBM Australia SWG Services

ONE voice for security.

IBM SECURITY SOLUTIONS

INNOVATIVE products and services.

IBM SECURITY FRAMEWORK

COMMITTED to the vision of a Secure Smarter Planet.

SECURE BY DESIGN

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2010. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.

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 Control: The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Netcool Performance Manager, ITCAM	
10.3.2: System acceptance 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.	IBM Security & Privacy Consulting Services, Tivoli Configuration Manager	
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 Control: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	Proventia IPS, IBM Managed Security Services, AppScan, DataPower, TAMeb	
10.4.2: Controls against mobile code 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.	Proventia IPS, IBM Managed Security Services, AppScan, DataPower, TAMeb	

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	IBM Security & Privacy Consulting Services, TFIM, DataPower	There needs to be a business agreement for federation of identities between two enterprises.
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.		
10.8.2: Exchange agreements	IBM Security & Privacy Consulting Services, TFIM, DataPower	
Control: Agreements should be established for the exchange of information and software between the organization and external parties.		
10.8.3: Physical media in transit	TotalStorage 3494, TS3100, TS3200, TS3500 Tape Library Systems, TSM, TKLM+encrypted media, IBM DLP services & partners	
Control: Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.		
10.8.4: Electronic messaging	DataPower, Lotus Notes, TAMeb, PGP	
Controls: Information involved in electronic messaging should be appropriately protected.		
10.8.5: Business information systems	IBM Security & Privacy Consulting Services	
Controls: Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.		

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	TAMeb, TFIM, DataPower, TSPM	
Control: Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.		
10.9.2: On-Line Transactions	TAMeb, TFIM, DataPower, TSPM	
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.		
10.9.3: Publicly available information	TAMeb, TFIM, DataPower, TSPM	
Control: The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.		

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.		