

C23 - IT Security Basics

Bryan Kissinger



September 21, 2009 – September 23, 2009

IT Security Basics

Bryan Kissinger, Director
PricewaterhouseCoopers LLP



September 21, 2009 – September 23, 2009



Discussion Topics

- Define information security, security functional areas and security layers
- Discuss the most pervasive security standards and regulations
- Define and discuss objectives, points of focus, controls and testing techniques related to IT Security audits and assessments
- Define and discuss maturity levels of information security organizations and the impact on the cost of compliance
- Discuss a number of case studies designed to help the audience translate theory into practice



COBIT Focus Areas

DS5

5.1-5.7 & 5.9-5.11

- Management of IT Security
- IT Security Plan
- Identity Management
- User Account Management
- Security Testing, Surveillance and Monitoring
- Security Incident Definition
- Protection of Security Technology
- Cryptographic Key Management
- Malicious Software Prevention, Detection and Correction
- Network Security
- Exchange of Sensitive Data



What is IT Security, Really?

Security is protection of people, property and information.

- *IT Security* addresses confidentiality, integrity and availability of information and supporting infrastructure.
 - LANs, WANs, Wireless (Network)
 - Operating Systems
 - Applications and Databases

So then...what isn't information security?



What isn't IT Security?

- Behavioral matters such as wasting time on the Internet or accessing inappropriate web sites
- Inappropriate use of computers such as passing chain letters and excessive web surfing
- Pornography
- Unsolicited e-mail
- Spam filter administration
- Pop-up browser ads
- other goofy stuff



Did you know?

- Approximately 80% of inappropriate access, data theft and other hacking incidents occur from within the organization
- Inappropriate access or escalated access results in the exposure to most internal hacks
- Unnecessary or unpatched services running on servers is the most common exploit used by external hackers
- The US-CERT (United States Computer Emergency Readiness Team) issues weekly cyber security bulletins related to discovered vulnerabilities and actions to mitigate the risk of the exposure

– <http://www.us-cert.gov/nav/t01/>

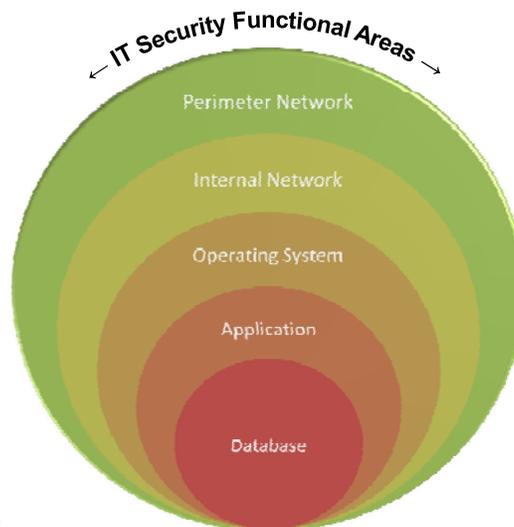


IT Security Functional Areas

<p>Security Organization & Management</p> <ul style="list-style-type: none"> • Define security program areas • Align with business & regulatory requirements • Manage investments for direct business benefit 	<p>Regulatory & Policy Compliance</p> <ul style="list-style-type: none"> • Consolidate business and regulatory requirements into defined information security policies and standards • Measure and monitor compliance
<p>Information Security Architecture</p> <ul style="list-style-type: none"> • Establish practices for designing and installing hardware • Incorporate security into the development process, • Create technology standards for the deployment of security services 	<p>Security Awareness & Education</p> <ul style="list-style-type: none"> • Educate, communicate, and periodically reinforce security roles and responsibilities • Create an environment of informed users
<p>Identity & Access Management</p> <ul style="list-style-type: none"> • Verify user identity • Control access to protected resources • Manage user's digital identities and provision access 	<p>Threat & Vulnerability Management</p> <ul style="list-style-type: none"> • Protect the enterprise from threats and vulnerabilities • Create an active defense posture and respond timely to potential breaches
<p>Privacy & Data Protection</p> <ul style="list-style-type: none"> • Control and monitor sensitive information within the organization 	<p>Physical Security</p> <ul style="list-style-type: none"> • Protect the physical assets of the corporation including information assets



IT Security Layers



IT Security Standards & Regulations

Standards*

- COBIT
- ISO 27000 Series: ISO 27001/2
 - Replaced ISO 17799
- NIST
- ISF

Regulations*

- PCI DSS
- HIPAA
- GLBA
- SOX
- FISMA
- EU Safe Harbor
- The California Information Practice Act or Senate Bill 1386
- Federal Energy Regulatory Commission
- International Traffic in Arms Regulation



*Not all-inclusive lists



IT Security Objectives

IT security objectives are based on the 8 functional areas described previously:

1. Security Organization and Management
2. Information Security Architecture
3. Identity and Access Management
4. Privacy and Data Protection
5. Regulatory and Policy Compliance
6. Security Awareness and Education
7. Threat and Vulnerability Management
8. Physical Security

The objective of most security programs is to ensure risks associated with the above areas are mitigated through the implementation of programs, controls and periodic assessments/audits.



IT Security Audit & Control Considerations

When designing an IT Security Assessment or Audit, there are points of focus, potential controls and test approaches that should be considered for each of the IT Security Objectives.

The following slides detail the most common focus areas, the controls that are most pervasively implemented and some potential testing techniques.



IT Security Audits/Assessments

Security Organization & Management

Points of Focus

- Has management designated the information security function based on an assessment of relevant information integrity risks?
- Has management considered the appropriate segregation of duties among personnel involved in the information security function?
- Is business unit management appropriately included in the design of the information security function from a data ownership perspective?
- Has management implemented personnel policies and procedures as well as clearly defined roles and responsibilities?



IT Security Audits/Assessments

Security Organization & Management

Potential Controls

- A member of the executive team should have ultimate responsibility for achieving the information integrity objectives of the organization.
- The functional security team should be designed to ensure an appropriate segregation of duties based on business requirements.
- Business unit management should “own” and approve all access to business data.
- Security responsibilities should be formally documented.
- All employees should be periodically reminded of their roles in achieving the organization’s information integrity objectives.
- Job applicants for sensitive security positions should be subject to background checks, reference checks, etc.



IT Security Audits/Assessments

Security Organization & Management

Testing Techniques

- Examine organization charts and inquire of IT and business unit management to determine the design of the security function.
- Observe evidence of segregation of duties during testing of the other aspects of the security focus areas.
- Examine job descriptions and security procedure documentation to determine whether information security roles and responsibilities are defined.
- Support conclusions about roles and responsibilities with observations during testing of the other aspects of the security functional areas.
- Examine evidence of the process used to ensure that all job applicants for sensitive positions are subject to appropriate background and reference checks.



IT Security Audits/Assessments

Information Security Architecture

Points of Focus

- Has Management considered the design of network assets keeping in mind tiering, segmentation and business purpose functions?
- Are security controls and countermeasures built into the SDLC process?
- Do standard build procedures exist based on the purpose of the hardware being deployed?
- How are changes to architecture design implemented and re-evaluated periodically?



IT Security Audits/Assessments

Information Security Architecture

Potential Controls

- The enterprise network is segmented and designed to ensure sensitive data and information assets are adequately protected.
- As new systems are being developed for production deployment, security controls are configured based on the function of the system.
- Standard build procedures exist based on the purpose of the hardware being deployed.
- The design of the network is periodically re-assessed to ensure it is architected most effectively to protect sensitive assets.



IT Security Audits/Assessments

Information Security Architecture

Testing Techniques

- Examine network topology maps to determine if the design of network assets is segmented or tiered appropriately.
- Review the SDLC process for implementing new systems to determine if security controls and countermeasures are being considered at the appropriate phases.
- Review any standard build procedures that exist determine if they are in keeping with the business uses of the hardware.
- Ask for the last review documents related to architecture re-assessments. Check to see if they were thoroughly performed and considered changes to the business.



IT Security Audits/Assessments

Identity and Access Management

Points of Focus

- Are user identities managed centrally?
- Is access granted based on job function / role?
- Has management established a standard and formalized process for granting access?
- Has management established a standard and formalized process for revoking access? Does the removal of access occur in a timely manner?
- Is access periodically reviewed to ensure appropriateness?
- Has management established a Public Key Infrastructure (encryption, key management, certificates, etc.)?



IT Security Audits/Assessments

Identity and Access Management

Potential Controls

- Central identity management tools (LDAP, Windows AD, reduced-sign-on tools, etc.) are leveraged to simplify IDM administration
- Role-based access control based on job function
- Formal and documented processes to grant and revoke access in a timely manner (including appropriate required approvals)
- Periodic review of access rights (especially to highly sensitive data/systems)
- Enterprise PKI program



IT Security Audits/Assessments

Identity and Access Management

Testing Techniques

- Examine central identity management tools (LDAP, Windows AD, reduced-sign-on tools, etc.) to ensure administration and configuration is appropriate
- Review existing access rights granted to each role
- Ask for screen shots / email trails documenting process of granting and removing access
- Select a sample of terminated users and review systems to verify access was removed
- Ask for evidence of periodic access rights reviews
- Review enterprise PKI program documentation. Select a sample of applications and determine if PKI program is being utilized as required by policy, or if acceptable alternatives are used.



IT Security Audits/Assessments

Privacy and Data Protection

Points of Focus

- Privacy program roles and responsibilities
- Privacy management framework
- Employee training and awareness
- Legal contracts and international compliance (EU Safe Harbor, etc.)
- User notification, awareness and consent (privacy policies, etc.)
- Gathering, use, storage and disposal of personally-identifiable information (PII lifecycle)
- Incident response processes (data loss incident, customer complaints, etc.)
- Controls in place to facilitate protection of personally-identifiable information



IT Security Audits/Assessments

Privacy and Data Protection

Potential Controls

- Privacy program roles and responsibilities are formalized and understood
- Privacy management framework is documented and approved
- Employee training and awareness program is established
- Legal contracts and international compliance agreements (EU Safe Harbor, etc.) are in place
- User notification, awareness and consent (privacy policies, etc.) processes are in place
- Allowable practices for the gathering, use, storage and disposal of personally-identifiable information (PII lifecycle) are documented and understood by staff
- Incident response processes (data loss incident, customer complaints, etc.) are formalized and in place
- Technical data protection controls are addressed by organization's security policy and standards and implemented



IT Security Audits/Assessments

Privacy and Data Protection

Testing Techniques

- Review privacy program roles and responsibilities; interview key stakeholders
- Review privacy management framework for completeness against industry standard practices
- Ask for evidence of employee training and awareness program
- Ask for a sample of legal contracts and international compliance agreements and interview stakeholders
- Review user/customer privacy policies against industry standard practices
- Analyzing practices for the gathering, use, storage and disposal of personally-identifiable information (PII lifecycle) and confirm compliance with privacy policies
- Review documentation for incident response processes (data loss incident, customer complaints, etc.)
- Conduct technical control gap analysis against organization's security policy and standards



IT Security Audits/Assessments

Regulatory and Policy Compliance

Points of Focus

- Has management identified all applicable information security regulations and implemented a plan for periodic review?
- Has management published a complete set of policies and procedures that support the information integrity objectives of the organization?
- Has management implemented a formal process to update security policy and procedure documentation on a regular basis?
- Has management established a process to ensure that IT and business users receive education and training regarding security policies and procedures, as well as their specific security responsibilities, on a periodic basis?



IT Security Audits/Assessments

Regulatory and Policy Compliance

Potential Controls

- Executive management has approved a complete set of information security policies and procedures that support the information integrity objectives of the organization as well as applicable regulations.
- A process to change the security policies and procedures is defined and documented, and all changes must be approved.
- The information security policies and procedures are readily available to all employees of the organization.
- IT and business users are all trained on information security policies and procedures when hired.
- A process to ensure security policies and procedures are followed (i.e., monitored).



IT Security Audits/Assessments

Regulatory and Policy Compliance

Testing Techniques

- Review applicable regulations and determine if a compliance function exists.
- Examine the documented information security policies and procedures to assess completeness.
- Examine evidence that a controlled process is in place to update the security policies and procedures.
- Observe the method of distribution and evaluate its effectiveness. Inquire of IT and business users to determine awareness of policies and procedures.
- Examine evidence of management's periodic information security reminders and of management's process for obtaining acknowledgements from all employees.



IT Security Audits/Assessments

Security Awareness and Education

Points of Focus

- What is the overall level of security awareness among employees?
- Has management established a security awareness and education program?
- Are new employees trained on security topics prior to starting their jobs?
- Are existing employees periodically re-trained on security topics?
- Do communication plans exist to alert employees to security emergencies?



IT Security Audits/Assessments

Security Awareness and Education

Potential Controls

- Resources dedicated to promoting security awareness and managing education program
- Periodic security reminders sent out to all employees
- Disciplinary program for security policy violations
- Security training for new employees
- Periodic security training for existing employees
- Security communication plan and mechanism to distribute security alerts



IT Security Audits/Assessments

Security Awareness and Education

Testing Techniques

- Interview security awareness and education resources
- Collect a sample of security reminders / communications
- Review disciplinary program for security policy violations
- Examine security training for new employees
- Examine periodic security training for existing employees
- Review security communication plan and mechanism to distribute security alerts



IT Security Audits/Assessments

Threat and Vulnerability Management

Points of Focus

- Is an Intrusion Detection / Prevention system in place? Is it configured appropriately?
- Are logs actively or passively monitored? Is a Security Event Monitoring system in place? What systems are in scope?
- How are malicious programs detected and quarantined? (Antivirus, spyware, etc.)
- How mature are the organization's incident response capabilities? Are incident response roles and responsibilities defined? Are the IR processes linked into the IDS/IPS, SEM, IT help desk, etc.?
- How are assets managed? Is there a "single source of truth"?



IT Security Audits/Assessments

Threat and Vulnerability Management

Potential Controls

- Intrusion Detection / Prevention system
- Active / passive log review, Security Event Monitoring system
- Antivirus, antispysware, etc.
- Formal and documented incident response procedures
- Assigned incident response roles and responsibilities
- Asset management system / CMDB



IT Security Audits/Assessments

Threat and Vulnerability Management

Testing Techniques

- Review Intrusion Detection / Prevention system configuration and related processes
- Review Active / passive log review and/or Security Event Monitoring system configuration and processes
- Review Antivirus, antispysware, etc. configuration. Select a sample of systems and verify tools are installed and functioning appropriately.
- Review formal and documented incident response procedures. Test incident response procedures periodically.
- Review asset management system / CMDB configuration. Select a sample of systems and verify they are represented accurately.



IT Security Audits/Assessments

Physical Security

Points of Focus

- How is physical access to Company buildings/sites restricted (consider any location where computer facilities are located, but also any locations connected to those facilities via the Organization's internal networks)?
- How is physical access to data centers restricted?
- How is physical access to remote data centers/server rooms restricted?
- How is physical access to wiring closets and other sensitive physical network locations/ components restricted?
- How is physical access to removable storage media (e.g., tapes, optical discs, etc.) restricted?
- How well secured is sensitive system documentation?



IT Security Audits/Assessments

Physical Security

Potential Controls

- All buildings/sites are protected using a card key access system.
- A formal security administration process is in place to grant, change and remove key card access.
- Access to the data center and remote data centers/ server rooms is protected by the card key access system.
- Wiring closets and other sensitive physical network locations/ components are subject to card key access restrictions.
- Removable storage media should be stored in a separate controlled area of the data center or in a vault.
- If hard copy sensitive system documentation is maintained, this documentation should be stored in secure file cabinets.



IT Security Audits/Assessments

Physical Security

Testing Techniques

- Observe the existence of card key readers at all entrances to the facility.
- Examine security administration requests for a sample of new employees with access to the facilities and data center for appropriate approvals.
- Examine a sample of key cards with access to the data center to ensure that access is commensurate with job responsibilities.
- Observe access controls at locations where storage media are maintained.
- Inquire of management and observe evidence of periodic reviews of physical access lists at off-site storage locations.
- Determine if periodic assessments of the physical access controls in place at the third-party locations are occurring.
- Observe controls over sensitive system documentation.



IT Security Program Maturity

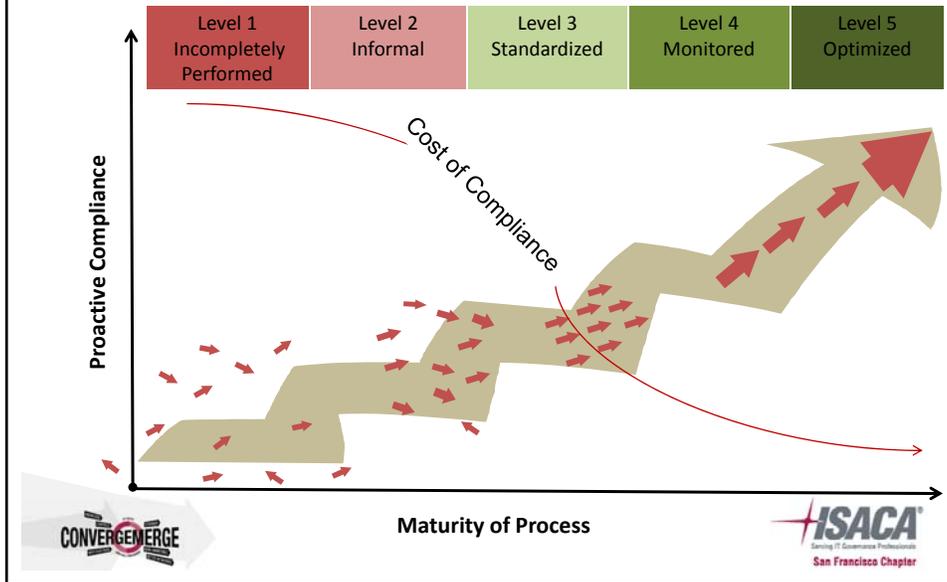
IT security program maturity can be plotted on the Capability Maturity Model (CMM) based on the definitions below:

1	Incompletely Performed	These processes are performed "Ad hoc" and may not have sustainable management
2	Informal	These processes are performed and managed but are not consistent throughout the organization
3	Standardized	These processes are managed and performed in a consistent manner throughout the organization
4	Monitored	Processes are consistently managed and quantitatively measured for performance consistency
5	Optimized	Process improvement is routinely incorporated to make the process more effective as a standard operating procedure



IT Security Program Maturity

Impact on the Cost of Compliance



Case Studies

Security Strategy Review - Green Tech Manufacturer

Scenario	Response	Result
Company experienced rapid growth over the last several years due to increased demand for its products and a major acquisition. Company recently separated from its parent company. Company also experienced an IT leadership change and several management positions were replaced. New IT leadership was not confident the company was taking appropriate measures to protect its assets, especially its trade secret manufacturing processes.	Company hired us to conduct an extensive review of its security program. A variety of assessment techniques were used, including interviews of key stakeholders, configuration testing, Data Loss Prevention tool pilot, penetration testing and physical security walkthroughs. The results of these various tests were reviewed from a high-level, holistic perspective, maturity ratings were developed and the top security concerns were identified.	By conducting a high-level review of the entire security program, as opposed to only a piece or certain systems, management was able to see the "big picture" and prioritize future security efforts based on risk rather than perceived need. Tests results provided "hard evidence" which IT leadership could use to build a business case for the management team.

Case Studies

Application Security Assessment Program Development – Pharmaceutical Distribution Company

Scenario	Response	Result
<p>Company's major business model depends very heavily on a large number of applications developed in house. These applications are all managed by different groups without major oversight by a central security organization. Company desired insight into the security risk of each of its major applications, and a standard methodology for measuring the security risk of applications going forward.</p>	<p>Company hired us to help them develop and pilot an application security assessment program. We met with all relevant stakeholders and documented business requirements. Leveraging industry standard practices, we developed a methodology that considered the application's function, its users, its supporting IT infrastructure, and other assessment results. The methodology was accompanied by an Excel-based assessment tool to help automated and standardize the assessment process.</p>	<p>Company benefitted in several ways:</p> <ol style="list-style-type: none"> 1. Gained immediate insight into the relative security risk of its major applications 2. Through stakeholder meetings, established positive new working relationships between various risk groups (security, IA, business units, etc.) 3. Established a standard assessment process that can be used going forward to track security risk over time



Case Studies

Identity Management System Implementation – Large Energy Client

Scenario	Response	Result
<p>Company planned to initiate a new remote access program which would give contractors working in the field the ability to connect to the Company network. Company needed assistance in creating the provisioning mechanism for this service, including the registration and de-provisioning of users. Company also needed guidance on the security concerns of sending sensitive user information through email in the registration process.</p>	<p>Company hired us to assess the security risks and concerns of this new program, and to implement an addition to their existing Identity Management (IdM) system. Using the expertise gained from prior implementations and a knowledge of the existing IdM structure, we designed appropriate provisioning and de-provisioning processes that facilitated the secure transmission of sensitive information. We also wrote custom code to integrate the new program into the central IdM system.</p>	<p>Company was able to move the new program into production on schedule. As a result, field technicians can now securely connect to the Company network and access critical company resources, increasing operational efficiency.</p> <p>The IdM integration facilitated an easy transition to the new program, as separate credentials are not required for access. In addition, there is no separate "one off" IdM tool to support as the central system was utilized. This user friendly solution minimized the impact of the new program on the helpdesk and IT support staff.</p>



Reference Material – “Good Reads”

[IT Auditing: Using Controls to Protect Information Assets](#) by Chris Davis, Mike Schiller, and Kevin Wheeler (Kindle Edition - Dec 22, 2006)

[Official \(ISC\)2 Guide to the CISSP CBK \(\(Isc\)2 Press Series\)](#) by Harold F. Tipton and Kevin Henry (Hardcover - Nov 14, 2006)

[Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition](#) by Stuart McClure, Joel Scambray, and George Kurtz (Paperback - Jan 5, 2009)

[CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50](#) by Kimberly Graves (Paperback - Feb 27, 2007)

[Computer and Information Security Handbook \(The Morgan Kaufmann Series in Computer Security\)](#) by John R. Vacca (Hardcover - Jun 5, 2009)

[Computer Security for Dummies](#) by Peter T. Davis and Barry D. Lewis (Paperback - Jun 1996) - Illustrated

