

InfoSec Support to Your Project Life Cycle – What We Can Do For You

PMI Breakfast Seminar

April 25, 2009

08:30 – 10:30 am



Precision Security Consulting

Aim of Presentation

- **To address key aspects of information security (InfoSec) so that PMs will know**
 - How to define "secure" deliverables that they produce
 - What they should expect from their InfoSec staff at each project stage
 - InfoSec deliverables in support of project success
- **To provide an opportunity for PMs to address their InfoSec concerns, questions and comments**

Session Outline

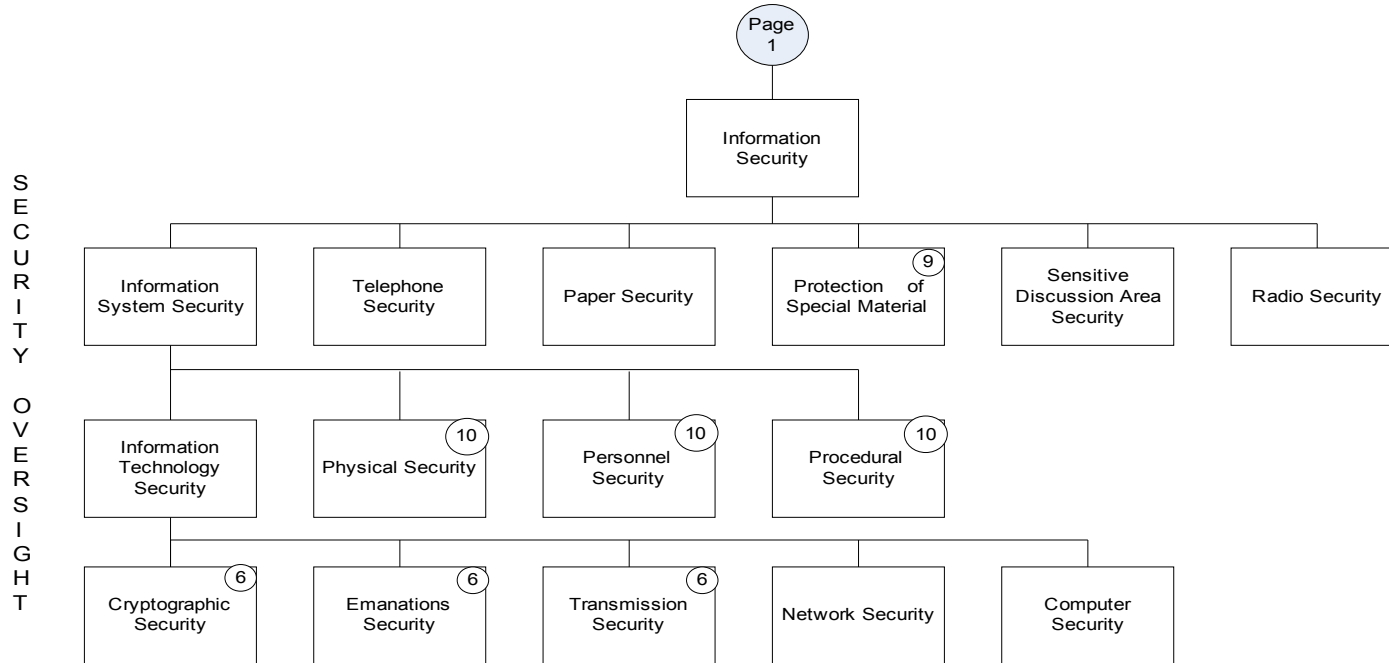
- **Key InfoSec Definitions and Concepts**
- **Mapping InfoSec Activities to the Project Processes**
- **Summary of InfoSec Activities**
- **Questions and Discussion**

Basic InfoSec Premises Applied to your Project

- **Security, like quality, must be built in from the outset so that it will be an enabler and not an impediment**
- **Your IT project deliverables have value and must therefore be protected**
- **Your IT project deliverables must be approved before they are put into operation**

Key InfoSec Definitions and Concepts - Scope of InfoSec

Security Awareness¹ Policy Functions of an Integrated² Departmental/Corporate Security Program (cont'd from Page 1)



NOTES:

1. Security Awareness for all is prescribed in Government Security Policy (GSP) February 2002, Sections 10.1 and 10.5.
2. GSP Section 10.1 prescribes the coordination of all security policy functions .
3. Not explicit in GSP but is part of industry standard integrated security programs and is noted in Canada's National Security Policy (NSP) April 2004, pp 7, 25-26.
4. Applies to both physical and logical environments .
5. Applies to all security policy functions.
6. Formerly Communications Security (COMSEC).
7. A component of information sharing in Section 10.2 of the GSP.
8. Includes security standards and procedures , security training and awareness in GSP Section 10.5.
9. This includes compartmented or proprietary information or other assets .
10. Coordinated with Corporate Security and applied to information systems .

Key InfoSec Definitions and Concepts - CIA Triad (plus A)

- **Confidentiality**
 - A security principle that ensures that information is not disclosed to unauthorized individuals
- **Integrity**
 - A security principle that ensures that information and systems are not modified maliciously or accidentally
- **Availability**
 - A security principle that ensures the reliability and timely access to data and resources by authorized individuals
- **Accountability**
 - All security-related actions are attributable to an individual

Key InfoSec Definitions and Concepts – Privacy

- **Level of protection afforded personal information (collection, use, distribution)**
 - Application of the CIA triad
- **Degree to which personal information may be divulged to the public, to the company, to selected employees, etc.**
- **Ensures intended recipients**

Key InfoSec Definitions and Concepts - Components of InfoSec Risk

- **Asset**

- Any product, software, data, hardware, administrative, physical, communications, or personnel resource within an IT system or activity that has *value*
- Critical Asset - Any asset whose compromise of CIA would result in a failure to provide functions or services essential to the business
- Intangible Asset - Asset that is not readily quantifiable
 - ❖ E.g. reputation, goodwill, market share, legal position

Key InfoSec Definitions and Concepts - Components of InfoSec Risk

- **Assets Include**

- Personnel
- Hardware
- Software
- Applications
- Information
- Media
- Materiel
- Infrastructure
- Policies, Standards, Guidelines, Procedures
- Culture

Key InfoSec Definitions and Concepts - Components of InfoSec Risk - Assets

- **Basic Premise**

- Measurable *value* therefore cost of loss
 - ❖ Quantitative and qualitative
- Injury test

- **Value/Worth**

- Value to data user (+), adversary (-)
- Acquisition, creation, development, maintenance, recovery replacement costs
- Lost opportunity
- Inherent or already established value
- Intellectual property, goodwill
- Time sensitivity
- Legal
- Moral, ethical

Key InfoSec Definitions and Concepts - Components of InfoSec Risk

- **Risk Assessment**
 - A study of mission, assets, vulnerabilities, threats, likelihoods, loss or impact and theoretical effectiveness of security measures
 - Both a process and interim result

Key InfoSec Definitions and Concepts - Components of InfoSec Risk

- **Threat**
 - A potential danger to information or any information system that can affect the CIA Triad
- **Vulnerability**
 - A system weakness or lack of something that could compromise the C-I-A Triad by being exploited by a threat agent
- **Risk**
 - Probability of a threat exploiting an IS vulnerability
 - ❖ Likelihood that threat will occur
 - ❖ Likelihood of adverse impact of exposure on asset
 - ❖ Severity of resulting adverse impact on asset
 - ❖ Chance of experiencing an undesirable outcome

Key InfoSec Definitions and Concepts - Controls, Countermeasures and Safeguards

- Risk-reducing measures that act to detect, prevent, or minimize loss associated with the occurrence of a threat or threat scenario
 - May be physical, personnel, technical or procedural
 - Resource-based or programmatic
 - Mitigate potential risk
 - Reduce *either* vulnerability *or* threat

Key InfoSec Definitions and Concepts - Residual Risk (R_R)

- The risk remaining after implementation of safeguards
- R_R is assumed by senior management
 - Accept
 - Mitigate
 - Transfer
 - Deny/Avoid

Key InfoSec Definitions and Concepts - Risk Equation

- $R = f(T * V * AV * O * I)$
- $R_R = \frac{f(T * V * AV * O * I)}{\text{Safeguards}}$

Key InfoSec Definitions and Concepts - InfoSec Risk vs. Project Risk

- **Project risks defined in terms of**
 - Quality
 - Budget
 - Schedule
 - Resources
- **InfoSec Risks are less precise, more flexible**
 - Risk Assessment a qualitative process
 - Types of safeguards chosen can affect budget
 - Risks can change with time
 - Competent InfoSec resources are best InfoSec risk mitigation vehicle
- **InfoSec Risks become project risks if customer's target R_R is not met**

Information Security & Risk Management

KEY DEFINITIONS & CONCEPTS

- **Certification**

- Comprehensive evaluation of the technical and non-technical security safeguards of an IS that establishes the extent to which a particular design and implementation meets a specified set of security requirements

- **Accreditation**

- Formal declaration that the IS is approved to operate in a particular security mode by using a prescribed set of safeguards.
- Official management authorization for operation based on the certification process as well as on other management considerations

Information Security & Risk Management

KEY DEFINITIONS & CONCEPTS

- **Information Systems Security Officer (ISSO)**
 - The person who is responsible to the operational authority for ensuring that security is provided for and implemented throughout the life cycle of IS from the concept development plan through the design, development, operation, maintenance, and secure disposal

Mapping InfoSec Activities to the Project Process- Initiating

#	PM Activity*	Supporting InfoSec Activity
1	Select project manager	Appoint Project Information System Security Officer (ISSO)
2	Determine company culture and existing systems	Determine R _R appetite of senior management
3	Establish project management office (PMO)	Establish a secure project environment
4	Collect processes, procedures and historical information	Determine IS security approval process
5	Divide large projects into phases	Determine required C&A deliverables
6	Identify stakeholders	Identify Facility staff, Certifiers, Accreditor
7	Document business need	Conduct mission analysis
8	Determine project objectives	Confirm protection requirements
9	Document assumptions and constraints	Document IS security assumptions and constraints
10	Develop preliminary project scope statement	Analyze preliminary security architecture and analyze IS security threats and vulnerabilities

*PMP Exam Prep, Rita Mulcahy, RMC Publications, Inc .2005

Mapping InfoSec Activities to the Project Process- Initiating

1. Appoint a project ISSO

- Training, education, experience
- Professional certifications
 - ❖ Certified Information System Security Professional (CISSP)
 - ❖ Certified Protection Professional (CPP)
 - ❖ Certified Information System Manager (CISM)
 - ❖ Certified Business Continuity Professional (CBCP)
 - ❖ Professional in Critical Infrastructure Protection (PCIP)
- Soft skills
 - ❖ Coordination
 - ❖ Mapping of business requirements into security requirements
- Maintaining a secure working environment (oversight)
- An advisor, not a decision-maker

Mapping InfoSec Activities to the Project Process- Initiating

2. Determine R_R Appetite of Senior Management

- Is a management decision, not a technical one
- May change as the situation dictates
- Need a R_R value for each of CIA

3. Establish a secure project environment

- Physical security and access control
- Cleared personnel
- Security policy and procedures
- Electronic access control
- Secure storage
- Separation of development, test and production
- Security awareness program and OPSEC

Mapping InfoSec Activities to the Project Process- Initiating

4. Determine IS security approval process

5. Determine required C&A deliverables

- Threat Risk Assessment (TRA)
 - ❖ Statement of Sensitivity (SoS)
 - ❖ Mission analysis
 - ❖ System description
 - ❖ Threat Assessment
 - ❖ Vulnerability Assessment (may include technical VA)
 - ❖ Risk Assessment
 - ❖ Assessment of existing safeguards
 - ❖ Determination of R_R
 - ❖ Recommendation on additional safeguards

Mapping InfoSec Activities to the Project Process- Initiating

5. Determine required C&A deliverables (contd)

- (Preliminary) Privacy Impact Assessment ([P]PIA)
 - ❖ Accountabilities for protection of privacy information
 - ❖ Privacy implications associated with trusted collecting (with consent), using, accessing, disclosing, accuracy, storing, disposing of sensitive personal information
 - ❖ Measures taken to date to mitigate system level privacy concerns arising from analysis of implementation and supporting procedures
 - ❖ Any additional operational security requirements to mitigate any additional privacy concerns
 - ❖ Basis for ongoing identification, evaluation and tracking of privacy concerns and their resolution throughout the system life cycle

Mapping InfoSec Activities to the Project Process- Initiating

5. Determine required C&A deliverables (contd)

- Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP)
 - ❖ BCP – continue or recover mission-critical business functions within recovery time objectives (RTOs) and recovery point objectives (RPOs) within Maximum Allowable Downtimes (MADs)
 - Non-technical
 - ❖ DRP – continue or recover mission-critical supporting IT within those same RTOs/RPOs
 - Technical

Mapping InfoSec Activities to the Project Process- Initiating

5. Determine required C&A deliverables (contd)

- Individual certification deliverables
 - ❖ Personnel security
 - ❖ Physical security
 - ❖ Technical security
 - Evaluated products (e.g., Common Criteria)
 - ❖ Procedural security

6. Identify Facility staff, Certifiers, Accreditor

- Accreditor
- Certification coordinators and certifiers
- Auditors
- Facility staff
- Corporate security (surveys)

Mapping InfoSec Activities to the Project Process- Initiating

7. Conduct Mission Analysis

- Part of TRA
- Confirm business lines supported by system, and protection requirements (CIA)

8. Confirm protection requirements

- Meet business requirements
- Minimize POF

9. Document IS security assumptions and constraints

- COIs
- Connectivity
- Data sensitivity and sharing

Mapping InfoSec Activities to the Project Process- Initiating

10. Analyze preliminary security architecture requirements

- Use of cryptography
- Separation of COIs, data sensitivity
- Availability requirements
- Initial threats and vulnerabilities based on initial CONOPS

Mapping InfoSec Activities to the Project Process-Planning

#	PM Activity*	Supporting InfoSec Activity
1	Create project scope statement	Confirm scope of architecture and C&A
2	Determine team	Confirm Certifiers and Accreditor
3	Create WBS and WBS dictionary	Create list of IS security safeguard deliverables
4	Create activity list	Create supporting IS security activities
5	Estimate time and cost	Estimate time and cost
6	Determine critical path	Support critical path IS security activities
7	Develop schedule	Develop IS security safeguard and C&A schedules
8	Determine quality standards, processes and metrics	Confirm expectations of Accreditor
9	Determine roles and responsibilities	Confirm roles and responsibilities of InfoSec staff
10	Risk Identification, risk analysis and response planning	Identification of project, deliverable and operational IS security risks
11	Determine what to purchase	Determine what IS security safeguards to purchase
12	Gain formal approval	Confirm security architecture and target R _R

*PMP Exam Prep, Rita Mulcahy, RMC Publications, Inc .2005

Mapping InfoSec Activities to the Project Process- Planning

1. Confirm scope of architecture and C&A
 - Refine as CONOPS is refined
 - Liaise with accreditation staff
2. Confirm Certifiers and Accreditor
 - Manage their expectations
3. Create list of IS security safeguard deliverables
 - Determine certification requirements
 - Liaise with developers
 - Continual verification of security risk and R_R

Mapping InfoSec Activities to the Project Process- Planning

4. Create supporting IS security activities
 - Project environment security oversight
 - C&A deliverables
 - Evaluation of secure products
 - Rules of connectivity
5. Estimate time and cost
6. Support critical path IS security activities
7. Integrate IS security safeguard development and C&A activities into project schedule
8. Confirm expectations of Accreditor (continual)

Mapping InfoSec Activities to the Project Process- Planning

9. Confirm roles and responsibilities of other InfoSec staff
 - Security architects
 - Product evaluators
 - Technical vulnerability assessors
10. Identification of project, deliverable and operational IS security risks
 - Project – system cannot be accredited
 - Deliverable – does not adequately protect CIA
 - Operational - mission failure due to breaches

Mapping InfoSec Activities to the Project Process- Planning

11. Determine what IS security resources and safeguards to “purchase”
 - Buy or build your ISSO, security implementers and InfoSec staff
 - Evaluated products or customized COTS
12. Confirm security architecture and target RR
 - Security architecture meets operational requirements
 - Senior management still agrees with target R_R

Mapping InfoSec Activities to the Project Process- Executing

#	PM Activity*	Supporting InfoSec Activity
1	Acquire final team	Confirm IS security contributors
2	Execute the PM plan	Coordinate the IS security solutions
3	Complete product scope	Populate the IS security architecture
4	Recommend changes and corrective actions	Recommend alternate IS security safeguards
5	Implement approved changes, defect repair, preventive and corrective actions	Respond to changes in target R_R or changes to security risk calculations
6	Follow processes	Execute the C&A process

*PMP Exam Prep, Rita Mulcahy, RMC Publications, Inc .2005

Mapping InfoSec Activities to the Project Process- Executing

1. Confirm IS security contributors

- Other ISSOs from connecting systems
- Security architects
- Trusted implementers
- Corporate security

2. Coordinate IS security solutions

- With accreditor
- With certifiers
- With connecting system ISSOs
- With system developers
- With testers

Mapping InfoSec Activities to the Project Process- Executing

3. Populate the security architecture

- Trusted integration and implementation

4. Recommend alternate IS security safeguards

- For cause (change to project scope or target R_R)
- Technical vs. non-technical
- To exploit emerging technology and evaluated products

5. Respond to changes in target R_R or changes to security risk calculations

- (Mission) assets, threats, vulnerabilities

6. Execute the C&A process

- Document gathering, production and QA
- Coordination

Mapping InfoSec Activities to the Project Process- Monitoring & Controlling

#	PM Activity*	Supporting InfoSec Activity
1	Measure against the performance measurement guidelines	Implement IS security solutions according to target R_R
2	Measure according to the management plans	Reassess IS security risk
3	Determine variances and if they warrant corrective action or a change	Respond to cost and time constraints with alternate IS security safeguards (temporary or permanent)
4	Scope verification	Target and actual R_R verification
5	Recommend changes, defect repair, preventive and corrective actions	Recommend alternate IS security safeguards or request amended R_R
6	Integrated change control	Assess R_R in architectural changes and recommend changes to safeguards

*PMP Exam Prep, Rita Mulcahy, RMC Publications, Inc .2005

Mapping InfoSec Activities to the Project Process- Monitoring & Controlling

- 1. Implement IS security solutions according to target R_R**
 - Trusted implementation
- 2. Reassess IS security risk**
 - Measure R_R associated with implementation, testing
 - Adjust according to changes in mission or risks
- 3. Suggest alternative IS security safeguards (variances and corrections)**
- 4. Verification of target and actual R_R (upon implementation of safeguards)**
- 5, 6. Assess new R_R after any project fixes**

Mapping InfoSec Activities to the Project Process- Closing

#	PM Activity*	Supporting InfoSec Activity
1	Develop closure procedures	Develop secure project environment closeout procedures
2	Confirm work is done to requirements	Confirm completeness of implemented IS security safeguards
3	Gain formal acceptance of the product	Achieve accreditation
4	Update lessons learned knowledge base	Update IS security risk and safeguard databases
5	Hand off completed product	Hand off accredited IS to operational ISSO
6	Release resources	... to fight another day

*PMP Exam Prep, Rita Mulcahy, RMC Publications, Inc .2005

Mapping InfoSec Activities to the Project Process- Closing

1. Develop secure project environment closeout procedures

- Secure disposal of IT media
- Archive or shred sensitive documentation
- Debrief project team
- Account for valued assets and return to stores

2. Confirm completeness of implemented IS security safeguards

- Correct implementation and functioning
- Review of audit logs
- POF is minimized

Mapping InfoSec Activities to the Project Process- Closing

3. Achieve accreditation

- Letter with conditions, rules of connectivity, accountability of operational authority

4. Update IS security risk and safeguard databases

- Yeah, right

5. Hand off accredited IS to operational ISSO

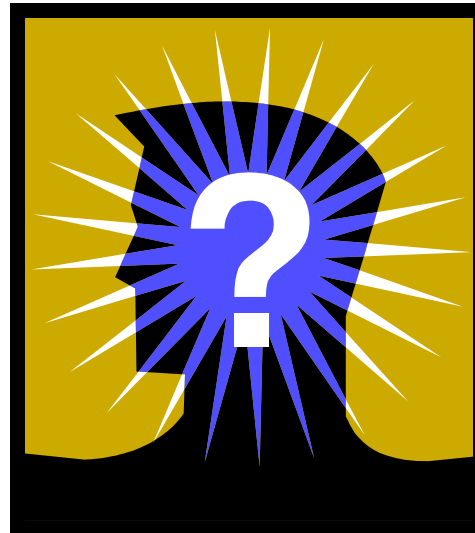
- Maintain conditions of accreditation
- Maintain accredited level of RR

6. Release resources

Summary of InfoSec Activities

- **Appoint competent ISSO**
- **Incorporate InfoSec risks into project risk management throughout**
- **Produce IS security deliverables**
 - TRA
 - PPIA, PIA
 - BCP/DRP
 - C&A evidence
- **Ensure deliverable systems can be accredited for secure operation**
 - Obtain accreditation
 - Handover to operational ISSO

Questions



Wayne Boone CD PhD CISSP CPP CBCP
CISM PCIP

wayneboone@rogers.com

(613) 863-2993