Information Security and Risk Management

Mike Smith

25/04/10 - Rev.20

Due ...

- **Diligence** - Do **Detect** - Steps to identify risks using best practices
- **Care** - Do **Correct** - Steps taken to correct identified risks to a minimum

Standards, Guidelines and Procedures

- Standards - Specify use of technology in a uniform way, compulsory
- Guidelines - similar to standards but not compulsory, more flexible
- Procedures - Detailed steps, required, lowest level
- Baselines - minimum standard and/or point in time

Risk Analysis

Steps

1. Assign Value to Assets
2. Estimate Potential Loss per Threat
3. Perform a Threat Analysis
4. Derive the Overall Annual Loss Potential per Threat
5. Reduce, Transfer, Avoid or Accept the Risk

- ALE = SLE x ARO = AV x EF x ARO
- Total Risk = threats x vulnerability x asset value
- Residual Risk = total risk x control gap
- Delphi Technique
  - Anonymous groupthink
  - Subjective only
- Qualitative
  - Eliminates $ amounts for cost benefit
  - Difficult to track
  - Standards not available
- Quantitative
  - Major project
  - Calculations are more complex
  - Laborious
  - More info gathering
  - Standards not available

Fault Logic Tree Analysis

- False alarms
- Insufficient error handling
- Sequencing or order
- Incorrect timing outputs
- Valid but not expected outputs

Failure Modes and Effect Analysis - FMEA

- Block diagram of system or control
- Consider what happens if each block fails
- Tabulate failures and effects
- Correct the design
- Have engineers review

Controls

- Administrative - Policies & Procedures
- Technical /Logical - Restricted Access
- Physical - Locked doors
- Preventative - prevent harmful occurrence
- Detective - detect after harmful occurrence
- Corrective - restore after harmful occurrence

C.I.A

- Confidentiality - prevent disclosure of data
- Integrity - prevent modification of data
- Availability - ensure reliable timely access

Classification

- Government - Unclassified/Sensitive/Confidential/Secret/Top Secret
- Commercial - Public/Sensitive/Private/Confidential

Risk Analysis Terms

- Asset - resource, product, data
- Threat - action with a negative impact
- Vulnerability - absence of control
- Safeguard - control or countermeasure
- Exposure Factor (EF) = % of asset loss caused by threat
- Single Loss Expectancy (SLE) = Asset Value x Exposure Factor
- Annualized Rate of Occurrence (ARO) - represents estimated frequency in which threat will occur within one year
- Annualized Loss Expectancy (ALE) - annually expected financial loss: ALE = SLE x ARO

Security Frameworks

Control Objectives for Information and related Technology (CobiT)

- Plan & Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Committee of Sponsoring Organizations (COSO)

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

Standards

- BS7799
- ISO 17799
- ISO/IEC 27000

Security Program

- Plan and organize
- Implement
- Operate and maintain
- Monitor and evaluate