BUILDING AN INFORMATION SECURITY RISK ASSESSMENT PROGRAM (WITH $0 BUDGET)

Kathy Doolittle CISSP, CISM, CEH
kathy.doolittle@onsemi.com

10.23.08
1. Background
2. Security risk assessments
3. Creating a repeatable, simple process - essentially at $0 cost (+ Labor, Existing Technology)
4. Examples of tools
5. Selling the idea to management
6. Reassess & Fix
Blueprints

- Focused on IT Security Risk
- Build it with little outlay of tools/$
  - More manual
  - Less complex
  - Good starting point
- Assess your needs (compliance, security, reporting)
Background
Background: Issues

- No security plans or risk assessment program in place; ad hoc tracking of issues
- No money, very limited staff
- Rare to no security/risk assessments for technology purchases, integrations, M&A
- Very limited security integration or involvement into IT requirements gathering
- Ad hoc security assessments for projects; limited risk assessment focused on SOX
Background: Goals

Main goal: Identify security risks in IT projects and manage the risks
Create a process for assessment
Communicate the need for Risk Management to management and peers
Integrate process into current process for least impact and increased chance of usage
Grow it
Security Risk Assessment*
What is Risk?

- hazard: a source of danger; a possibility of incurring loss or misfortune
- adventure undertaken without regard to possible loss or injury
- exposure to a chance of loss or damage

Safety is a myth. Risk is reality. Fear is the mind killer. Seize the day. Take the road less travelled. Dare to be different. Nothing ventured, nothing gained. The adventure is within. Boldness has no price. Take the first step.
What is Security Risk?

**Business Risk**
Factors that may cause a failure to meet a company’s objectives
- Growth risk
- Technology risk
- Marketing risk
- Financial risk
- Team/Management risk

**Project Risk**
Factors that may cause a failure to meet a project’s objectives
- Inexperienced personnel
- New technology
- Time constraints
- Budget
- Dependencies

**Security Risk**
Factors that may cause a failure to meet a company’s risk acceptance level or regulatory requirement
- Impacts to Confidentiality, Integrity, Availability due to vulnerabilities & threats

**ACCEPT**: Implement Workarounds -- Reactionary - Unfunded
**MITIGATE**: Implement Some Preventive Controls --- Partially Funded
**TRANSFER/AVOID**: Implement Strong Preventive Controls &/or Insurance – Fully Funded
Why Do We Assess Security Risk?

Money Spent

Security Provided

Spend Priority

Allocate Resources (people & Tech)

Meet Regulatory Requirements

Identify Security Protection Gaps

Understand Threats
What an Assessment Identifies

**Asset**
What are you trying to protect?

**Threat**
What are you afraid of happening?

**Vulnerability**
How could the threat occur?

**Mitigation**
What is currently reducing the risk?

**Impact**
What is the impact to the business?

**Probability**
How likely is the threat given the controls?

**Well-Formed Risk Statement**
Example: Assessment Outcomes

- Proactively identify risks that are posed to systems and data
- Quickly identify and prioritize high risk projects
- Assure adequate planning, scoping, and prioritization for new security services or protection methods

Outcome:
- Fully understand & communicate company risk posture & status
- Identifies risks to core systems when integrating new systems
- Ability to measure risk and show value of security projects
- Holistically manages risk in a global infrastructure
- Manages risk in a repeatable way for compliance requirements
Creating a Repeatable Process
Creating the Process: Gap Analysis

Drivers & Outcomes
- Drivers: Regulatory, best practices, certifications, business
- Outcomes: What do you want/need to meet drivers?

Components
- What do you have & what do you need (people, processes, technology)
- What is your timeline and who will be involved?
- Do you have any funds? Do you have a sponsor?

Interaction
- Who are the stakeholders? Educate or must sell?
- Where are points of interaction for process?
Use What You Have

Technology
- Office type apps or open source (databases, spreadsheets, presentations)
- SharePoint
- Web servers
- Security VA programs
- Maturity Modelers (Gartner)

Processes
- Methodologies (SDLC, MSF, other Project Lifecycles)
- Purchase Approvals
- Change Controls
- Project Approval Process
- Communication paths (mgt meetings, HR, legal, audit committees
- Training (brown bag)

People
- Stakeholders
- Security, Audit
- Board of Directors
- Communications Director
- Application Developers
- Project Managers
- C-Level Backing

Your wits, your intelligence, your charm, your experience, your personal ‘hammer’
Example: RA in the Project Lifecycle

- **RAD (Risk Acceptance Document), if necessary**
- **Stabilizing Phase Checklist Approved**
- **Developing Phase Checklist Approved**
- **Envisioning Phase Checklist Approved**
- **Planning Phase Checklist Approved**
- **Initial Risk Questionnaire (IRQ) for all projects**
- **RISC plan (Security Plan) for high risk projects**
Initial Process

All Projects

IRQ - Information Risk Questionnaire
Project Managers or Sponsors

ONLY Moderate & High Risk IRQ Scored Projects

RISC Plan – Risk & Information Security Controls Plan
Information Security Analyst (+ project architects)

ONLY Projects with Critical and High Risks to Accept

RAD – Risk Acceptance Document
Project Managers & Sponsor
## Identify the Focus & Priority

<table>
<thead>
<tr>
<th>Focus</th>
<th>Priority</th>
</tr>
</thead>
</table>
| - Where will you focus out of the gate and why?  
  - Regulatory systems  
  - Security systems  
  - New technology or processes  
  - Foundational systems  
  - Critical processes  
  - Application development | - Set achievable goals  
- Set achievable timelines and stick to them  
  - Quarterly & Yearly  
  - System Focus  
- Prioritize based on what you can do with limited budget and personnel |

- Use drivers & desired outcomes to help you focus
Think in Terms of Standardization

- **Documentation**
- **Processes**
  - Integration points
  - Standard Assessment methods
    - Policies, standards (internal, best practices, etc)
    - Conducting the assessment
    - Project Risk Levels
- **Follow up**
- **Tools**
- **Communication methods**
- **Terminology**
- **Metrics**

<table>
<thead>
<tr>
<th>Project Risk Levels</th>
<th>Slight &lt;28 points</th>
<th>Guarded 29-33 points</th>
<th>Moderate 34-39 points</th>
<th>High &gt;40 points</th>
</tr>
</thead>
</table>

Make It Repeatable

Defined: Integration Points

Defined: methods of communication

Defined: processes for assessment

Defined: path for fix/assess/fix...

Standard documentation
Create the Process

- Focus on your main priorities & goals
- Prioritize your SRA process over time
- Create standard templates & documents
- Use existing corporate processes & add to them
- Keep it easy to use
- Test it out prior to deployment
- Re-evaluate over time (quarterly, yearly)
Examples

- The IRQ (Information Risk Questionnaire)
- The RISC (Risk and Information Security Controls)
- The RAD (Risk Acceptance Document)
Information Risk Questionnaire

The IRQ Requirements

- Asks key questions to score risk
- Extremely easy to use by non-security (or audit) personnel
- Quick (~ 10 minutes at most)
- Implemented in early stage of project lifecycle
- Low cost (.xls and stored on SharePoint)
Risk & Information Security Controls

- Repeatable process
- Standardize method to limit risk and control types, ability to add types
- Project, Foundational, Ad Hoc Plans
- Low cost (Access Database) to create & maintain (but can be ported later)
- Ability to imbed design documents
- Ability to report based on risks, controls, outstanding issues, foundation & project plans
- Multiple associations between risks & plans allowed
RISC Database Schema Exam

**Project List**
- Project Register #
- Name
- Lead
- Description
- IRQ Score
- RISC Plan Needed?
- Follow-up Review Date

**Risk List**
- Risk Short Description
- Category
- Likelihood
- Inherent Impact
- Risk Level
- Suggestion/Recommendation

**Standards**
- Standard Name
- Type

**Schematics**
- Schematic Name
- Version #
- Date
- Author

**Foundation Plans**
- Plan #
- General System
- Version #
- Date
- Author

**Controls**
- Control Short Description
Management signoff on High and Moderate (year 2) Risks
Documented
Provides means to communicate on security & risk
Provides means to “include security early on in a project”
## Process Development: Lessons Learned

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Development</strong></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Really understand the processes to integrate with</td>
</tr>
<tr>
<td>2.</td>
<td>Get to input from users</td>
</tr>
<tr>
<td>3.</td>
<td>Combine forces for IRQ development</td>
</tr>
<tr>
<td>4.</td>
<td>Limit amount of new documents or processes</td>
</tr>
<tr>
<td>5.</td>
<td>Get a sponsor</td>
</tr>
<tr>
<td>6.</td>
<td>If you have no money, you can achieve a repeatable process, but limit your focus &amp; first year goals</td>
</tr>
<tr>
<td>7.</td>
<td>Start focused and build from there</td>
</tr>
<tr>
<td>8.</td>
<td>If you have limited personnel, make sure they are fully trained in process and goals for each year</td>
</tr>
</tbody>
</table>
Training Users

- Introduce Security Risk
- Identify the process (e.g. Slide 18)
- Explain impact to them
- Require training for IRQ
- Keep an open dialog
  - Have a Wiki (or FAQ site)
  - Have lots of online material
- Touch base and get feedback
Selling Security Risk Management
# Selling the Idea to Management

## What
- Introduce idea of *Security Risk*
- Be clear on impact to users and processes
- Show high level plan
- Focus on immediate impact & deliverables
- Don’t oversell (too many graphics, metrics, charts)

## How
- Use compliance requirements, security audits/VAs
- Grab metrics
- Focus on goals of assessments
- Advance simple ideas regarding process inclusion
- Define impact of process at high level
- Don’t forget industry practices
Selling – Go In Knowing:

How: Process Will Integrate with Existing Business Processes

Who: Key Users

What: Cost, Effort

What: Deliverables

When: Timeline

What: Projected Outcomes
Review & Reassess

- IRQ Scoring
- # of Projects Using Process
- RISC Plan Identification, Scoring Values & Validity
Next Logical Steps

- Shore up weak points in process or assessments
- More Project Types (M&A, Applications, Partners)
- Increase RISC Plans for more types

<table>
<thead>
<tr>
<th>Slight</th>
<th>Guarded</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;28 points</td>
<td>29-33 points</td>
<td>34-39 points</td>
<td>&gt;40 points</td>
</tr>
</tbody>
</table>

- Increase RADs for Moderate (add to Critical/High)
- Globalize Process
- Require training 2x year for Security Assessors
- Give Audit/Compliance & Management Updates on Progress
Lessons Learned
My Lessons Learned

What I Wish I Knew Then

- M&A Issues
- Expect Pushback - IT
- Running Aground on other Processes
- Sell, Sell, Sell
- Don’t stop communicating
- Take Compliance & Audit to lunch - often