



Taking Information Security Risk Management Beyond Smoke & Mirrors

Evan Wheeler
Omgeo

Session ID: GRC-107

Session Classification: Intermediate

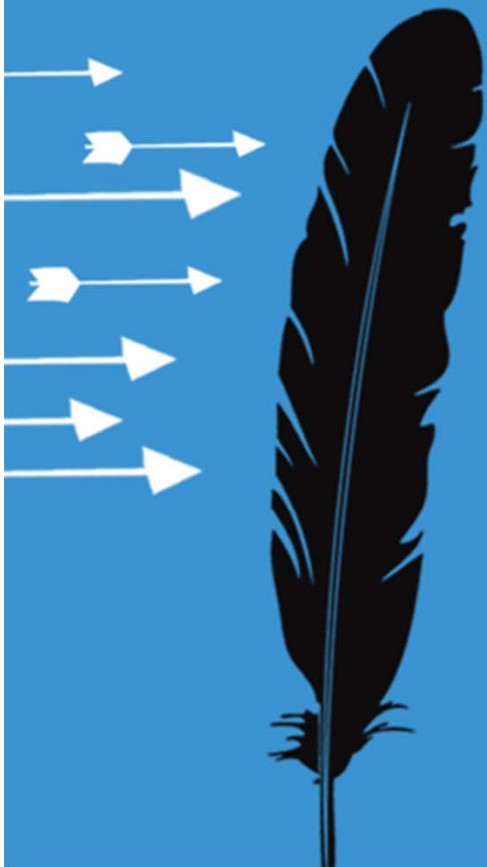
RSACONFERENCE2012

Session Agenda

- Designing a Risk Program
- Prerequisites for a Risk Management Program
- Program Roadmap



Designing a Risk Program



Common Perception of Risk Management

Right Now	Next 36 Hours		
 Partly Cloudy 34°F Feels Like: 29° Get FREE weather on your desktop	Today  Partly Cloudy 43° High	Tonight  Clear 20° Low	Tomorrow  Sunny 42° High
Past 24-hr: Precip: 0 in Snow: 0 in	Chance of Rain: 10%	Chance of Snow: 0%	Chance of Rain: 0%
Wind: From NW at 5mph	Wind: NNW at 8 mph	Wind: NNE at 4 mph	Wind: ENE at 3 mph
Through 3pm: Partly cloudy with temperatures rising towards the low 40s. Winds NW at 10 to 15 mph.	Some clouds this morning will give way to generally sunny skies for the afternoon. High 43F. Winds NNW at 5 to 10 mph.	Mainly clear. Low around 20F. Winds light and variable.	A mainly sunny sky. High 42F. Winds light and variable.



Lacy Atkins / The Chronicle



Program Goals

- Empower Business Units to Identify & Remediate Risks
- Help Prioritize Remediation Tasks
- Educate the Organization Regarding Real Threats & Weaknesses
- Increase Visibility and Capability to Track Risks
- Improve the Consistency of Risk Assessment Approaches



Program Goals

- **Empower Business Units** to Identify & Remediate Risks
- Help **Prioritize** Remediation Tasks
- Educate the Organization Regarding **Real Threats & Weaknesses**
- **Increase Visibility** and Capability to Track Risks
- Improve the **Consistency** of Risk Assessment Approaches



Program Lifecycle

Phase 2 - Risk

- Policy Exception Acceptance
- Mitigation Plan Tracking Process
- Risk Reporting
- Certification
- Security Scanning / Penetration Testing

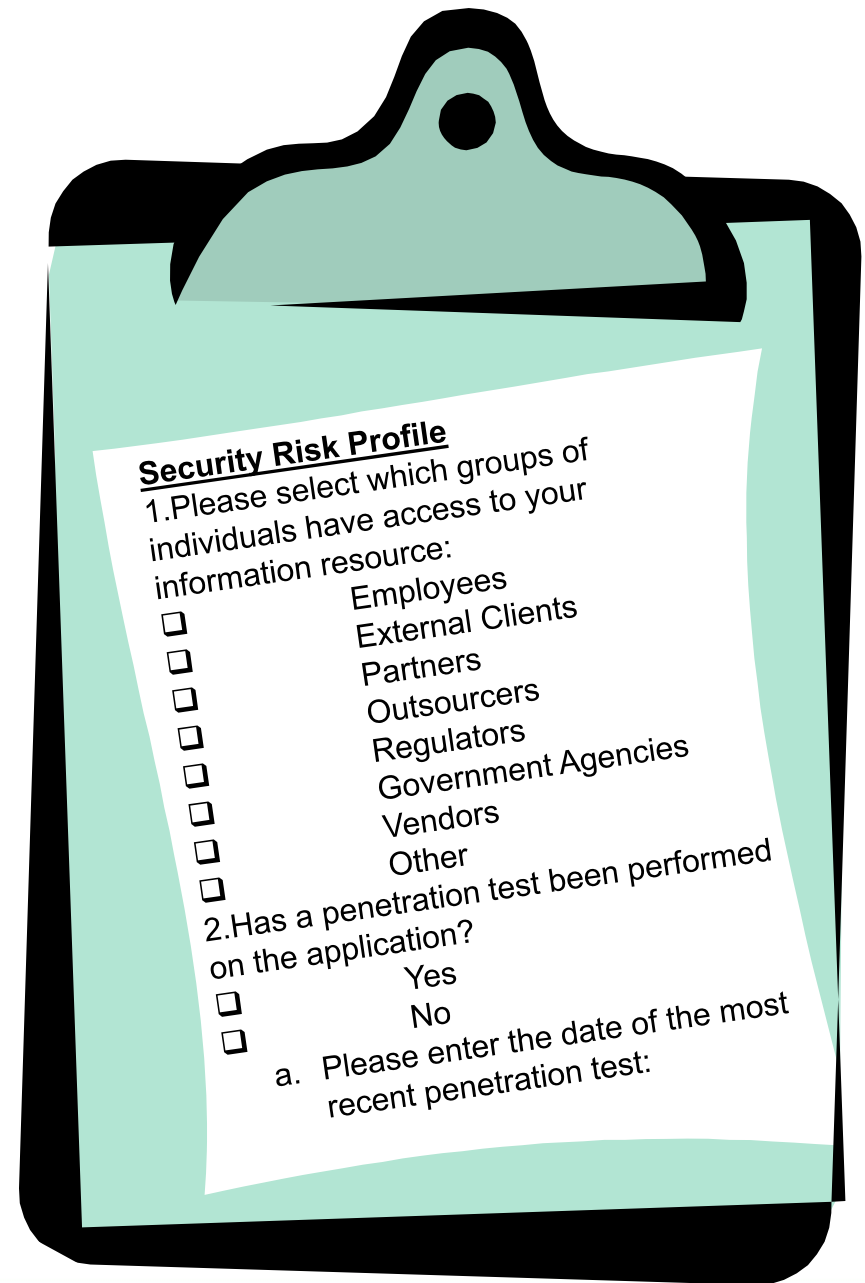
Phase 3 - Risk Monitoring

- Risk Register / Inventory
- Re-Assessment Schedule
- Security Event Monitoring
- Incident Response & Tracking
- Independent Audit Program
- Key Risk Indicators Reporting
- Risk Training & Awareness Program

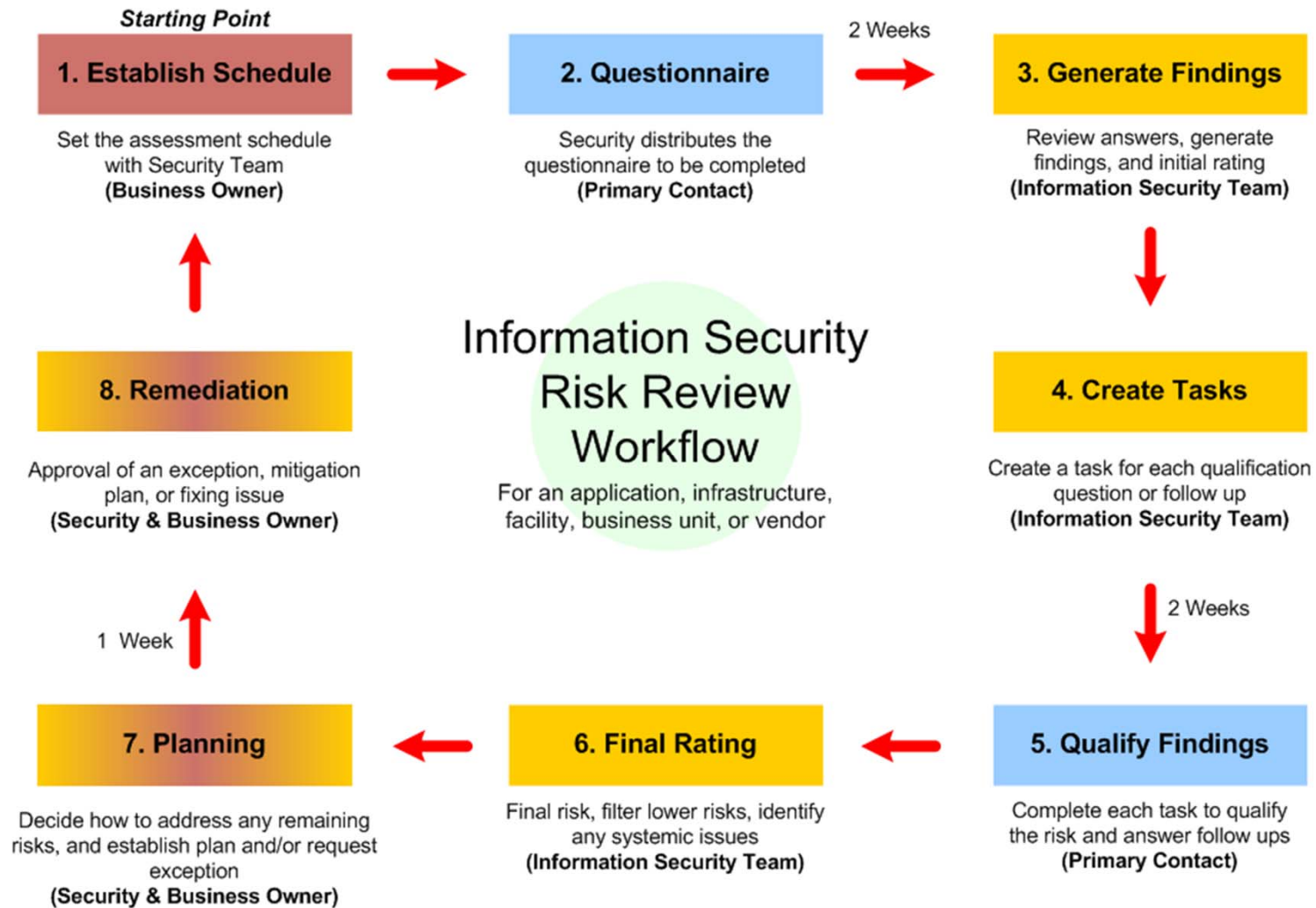


Resource Profiling

- Identify critical assets
- Rate their importance or impact to the organization, and relative to each other
- Start with a basic scale (L, M, H)
- Application, System, or Environment

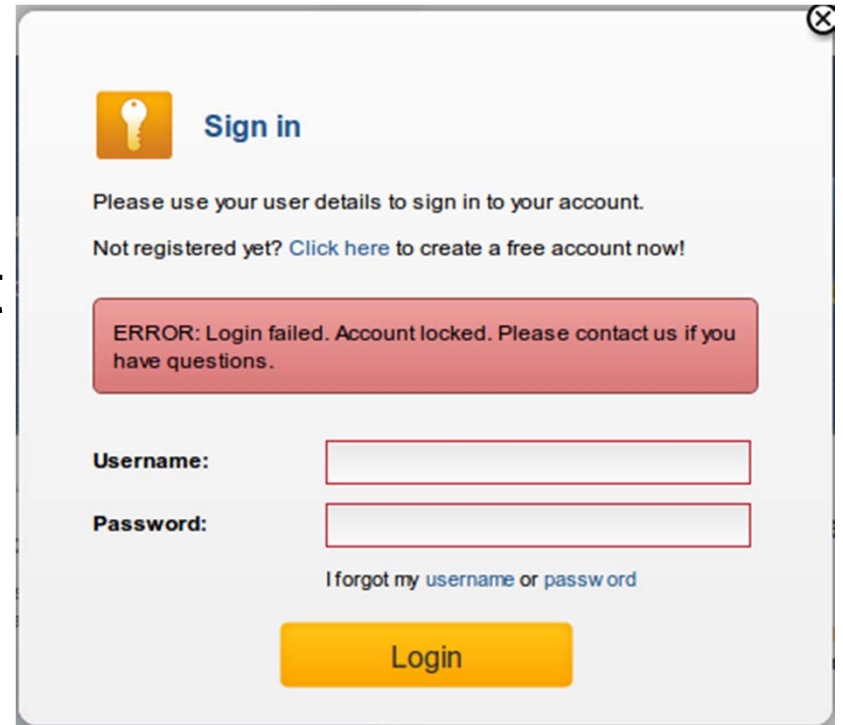


Looking at the Internal Gaps



Not an Audit

- E-Commerce site
- Current Password Lockout Policy:
 - 3 attempts before lockout
 - Unlock requires administrator
- Proposed change:
 - 5 attempts before lockout
 - Automatic unlock after 15 minutes

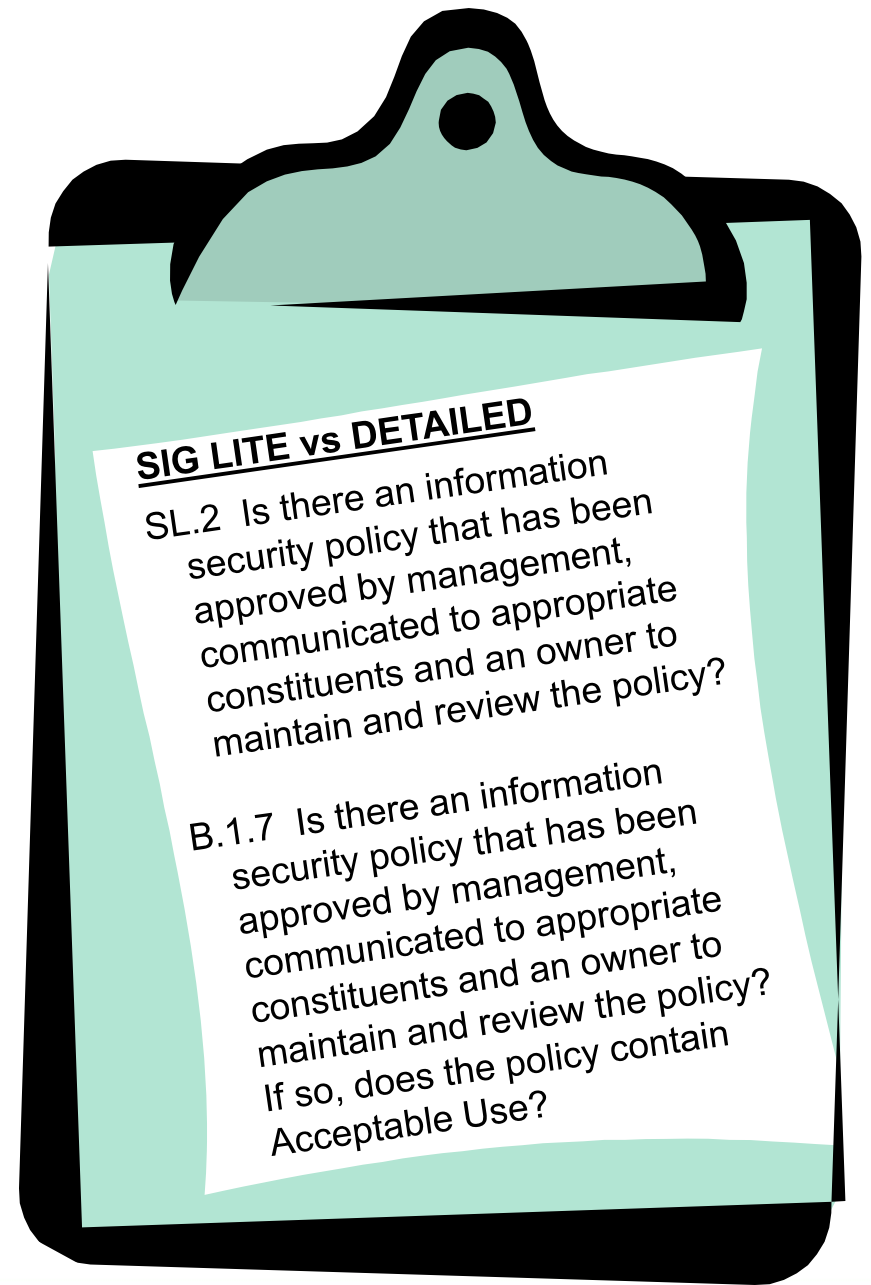


The screenshot shows a web application login interface. At the top left is a yellow key icon next to the text "Sign in". Below this, a message reads: "Please use your user details to sign in to your account." followed by "Not registered yet? [Click here](#) to create a free account now!". A red error box contains the text: "ERROR: Login failed. Account locked. Please contact us if you have questions." Below the error box are two input fields: "Username:" and "Password:". Below the password field is a link: "I forgot my username or password". At the bottom is a yellow "Login" button.



Going External

- Security Risk Profile
- Architectural Review
- Questionnaire
 - Common Format
 - Tailored by Risk Profile
 - Linked to Internal Policies/Standards
- On-Site Review
- Example: FedRAMP Security Controls list



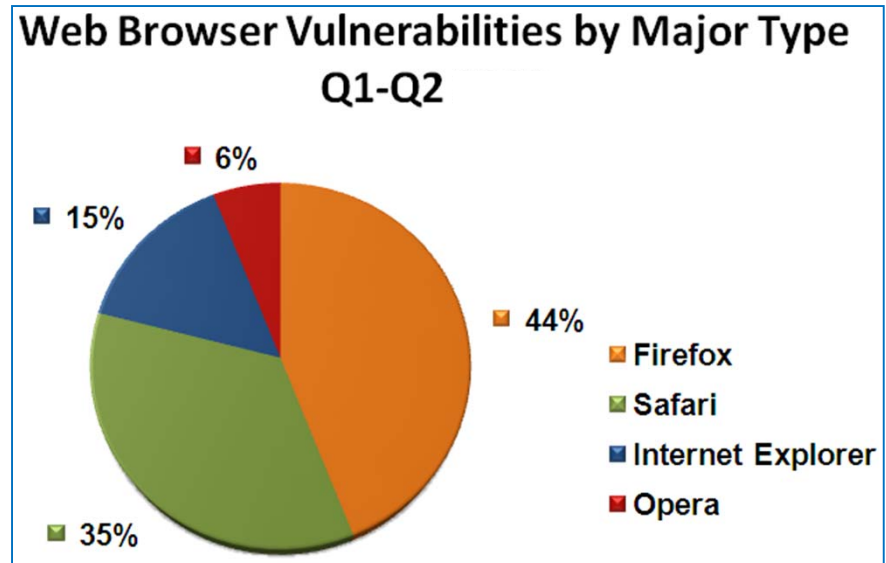
Vendor Review Schedule Example

Vendor/Service	Risk Sensitivity	Last Assessment Date	Risks Discovered in Last Assessment (400 Questions)	Next Assessment Date
Vendor A	High	SIG Detailed 11/23/2010	Critical: 0 High: 0 Moderate: 15 Low: 4	SIG Level 2 12/01/2012
Vendor B	High	SIG Detailed 2/17/2010	Critical: 1 High: 5 Moderate: 43 Low: 12	SIG Detailed 03/01/2011
Vendor C	Moderate	SIG Level 1 8/11/2009	Critical: 0 High: 11 Moderate: 61 Low: 7	SIG Level 1 09/01/2011

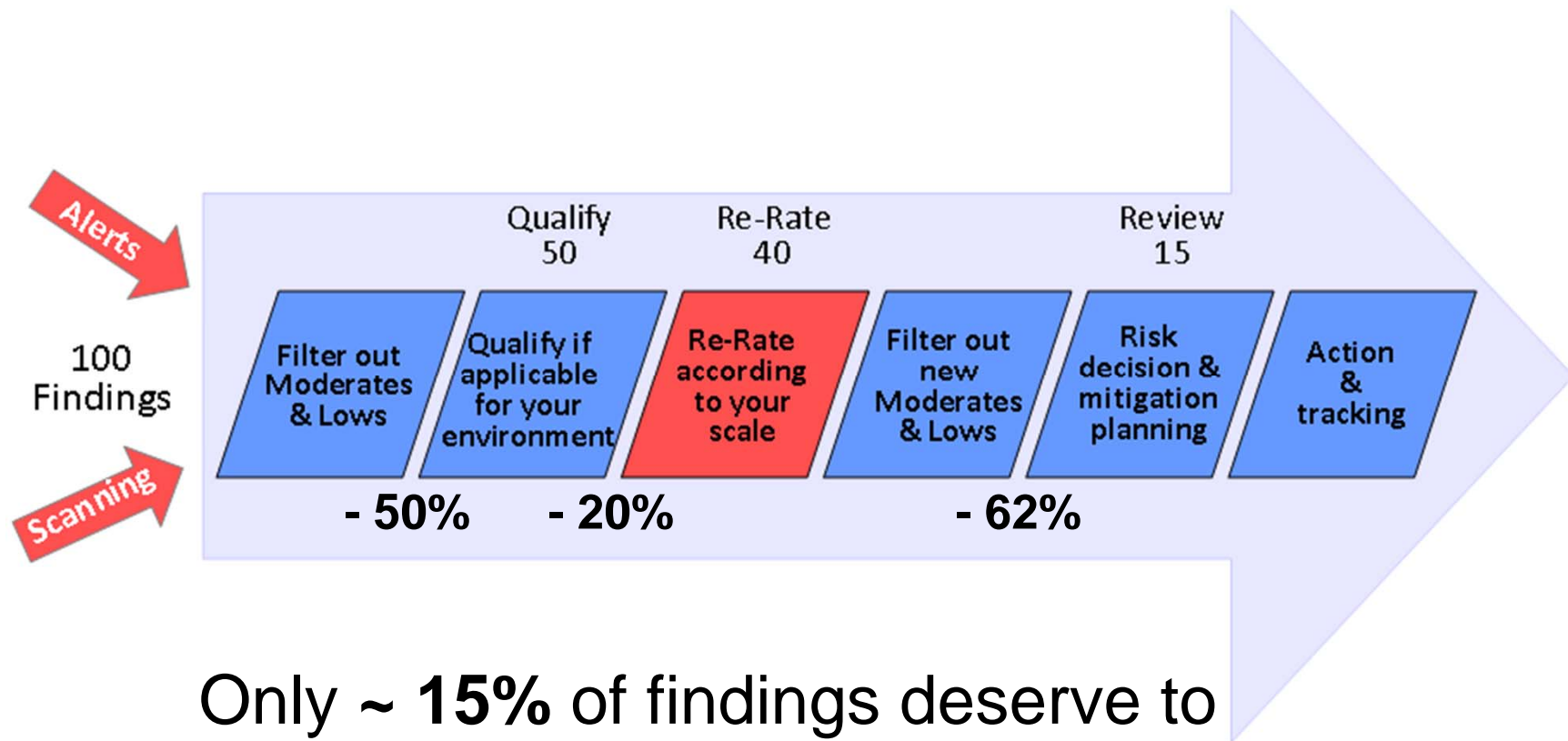


Threat & Vulnerability Management

- Risk Identification
 - Security Scanning
 - Penetration Testing
- Risk Response
 - Remediation SLA
 - Presenting to Metrics to Management
- Risk Monitoring
 - Monitor Advisories
 - Scanning & Testing Schedule



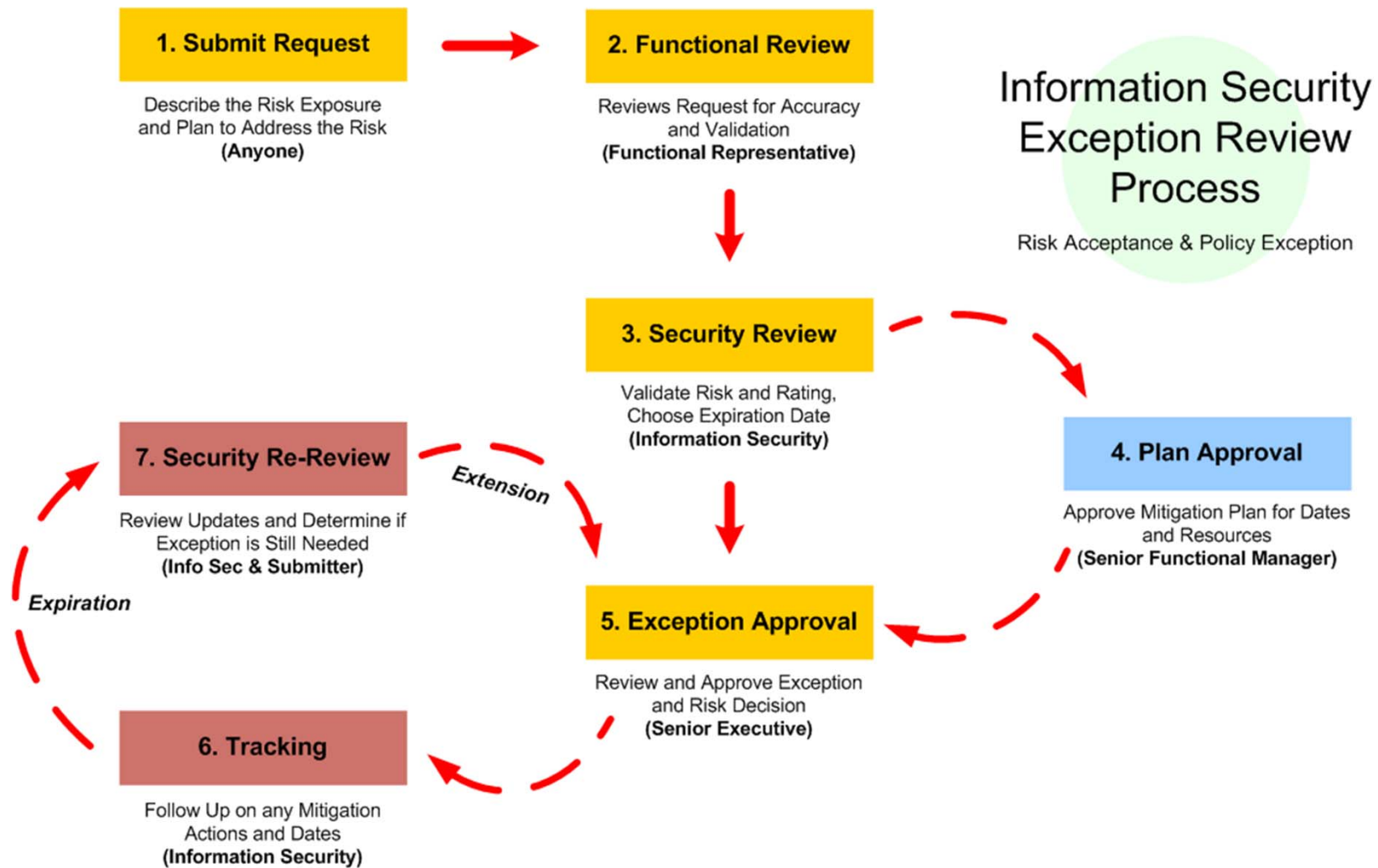
Filtering is Your Friend



Only ~ **15%** of findings deserve to be addressed the first time through



Oversight & Tracking

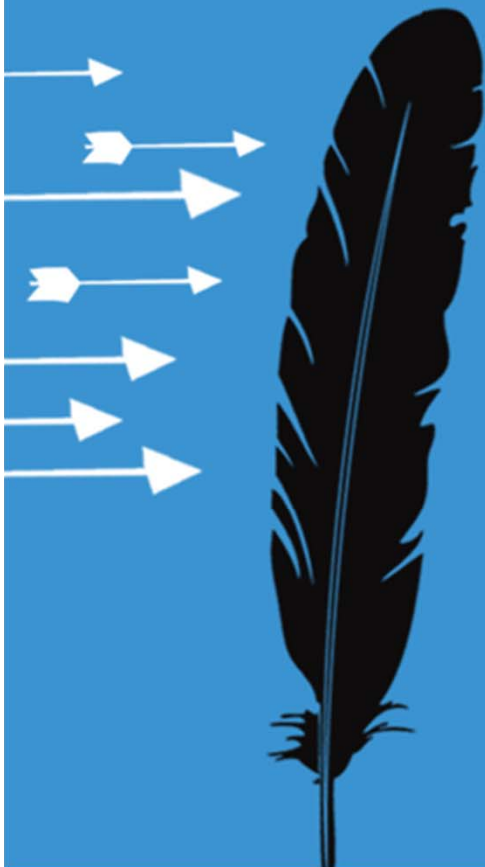


Steal What's Out There

- NIST
 - High-level approach evolved into C&A solution
 - Comprehensive lifecycle
 - Automated implementations are successful
- OCTAVE Allegro
 - Detailed worksheets & questionnaires
 - Best suited for projects and one-time assessments
- FAIR
 - Detailed quantitative and probabilistic method
 - May be overwhelming for novices without integration into a tool



Prerequisites for a Risk Management Program



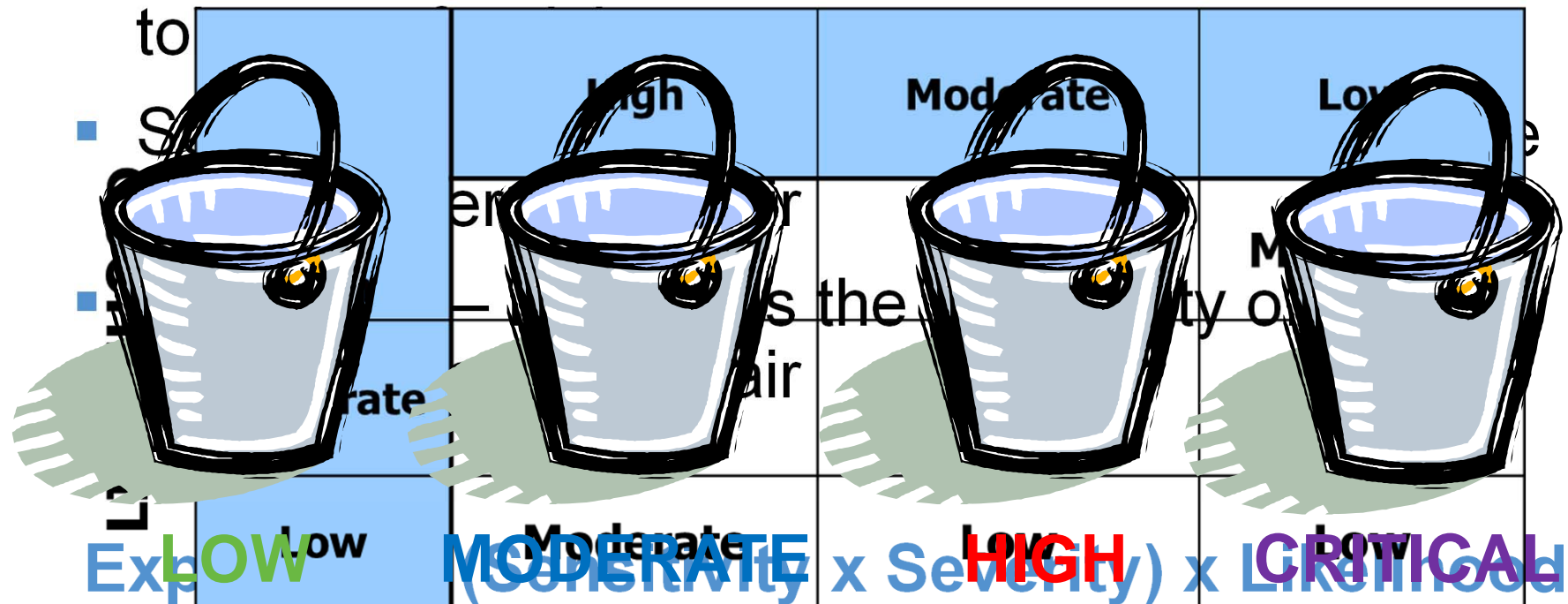
Program Prerequisites

- Security Policies, Standards and Baselines
- Information Resources Inventory
- Common Risk Formula
- Enterprise Risk Committee
- Mapping of Risk Domains to Business Objectives



Sensitivity-Based Risk Model

- Sensitivity – a value relative to the resource's to



High – Corrective action must be implemented in 30 days

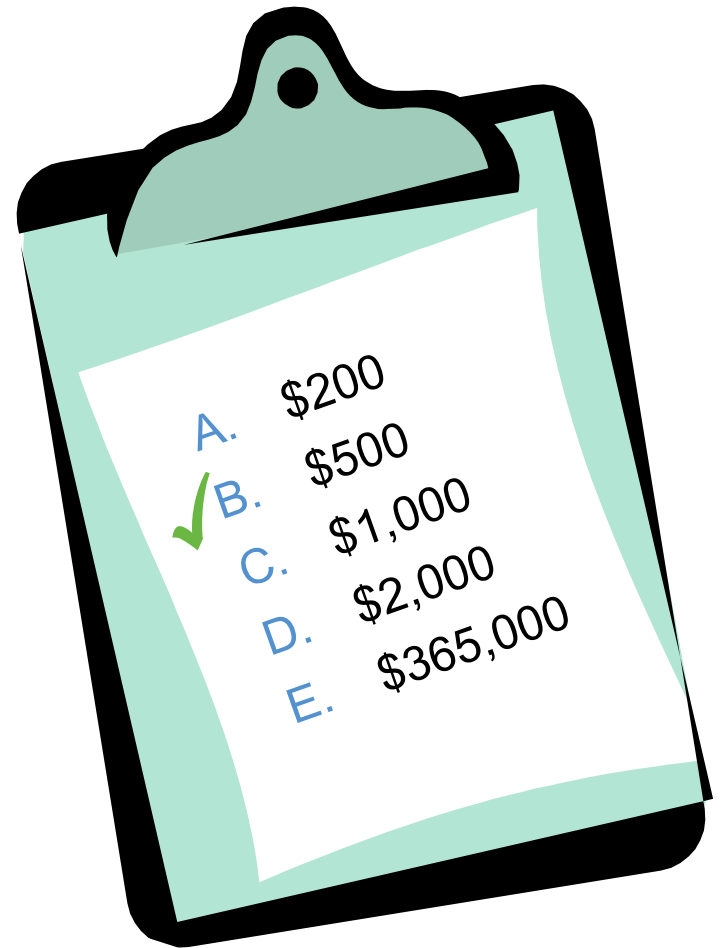
Moderate – Corrective action must be implemented in 90 days

Low – Corrective action must be implemented in 1 year



Self-Assessment

- Calculate the Annual Loss Exposure (ALE) given the following details:
 - Each laptop in your company costs \$1,000 to replace
 - Based on your asset tracking records, you have estimated 1 laptop gets stolen every 2 years
 - There is no other value associated with these laptops
- Based on this scenario, what is the ALE for this risk?



Applying the Textbook Risk Approach

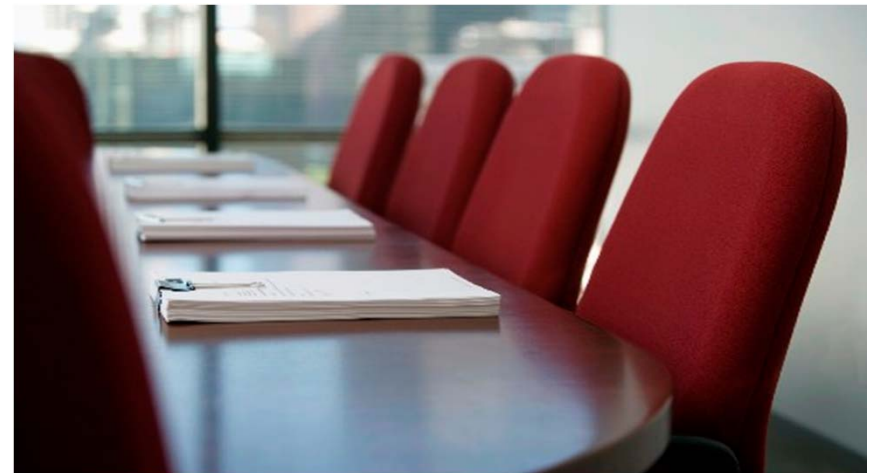
Now try to calculate the ALE of these scenarios:

1. Backup tapes with sensitive data are transferred to an offsite storage facility in the back of an intern's car once per week, and all data is in cleartext
2. All Internet links are serviced by a single ISP
3. Multiple vulnerabilities in Adobe Reader 9 and Acrobat 9 could allow remote attackers to crash the application or potentially control affected systems.



The Big Picture

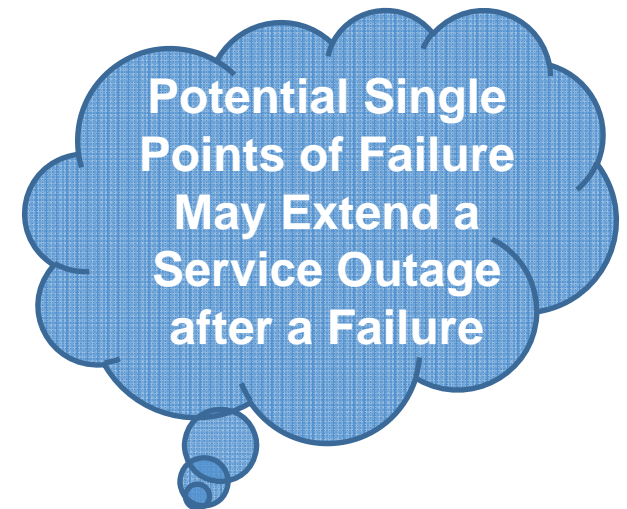
- Enterprise Risk Committee(s)
 - Looks at risks across the entire organization
 - Information Security is just one member
 - Focus on only the highest level risks
 - Often systemic or thematic risks are highlighted
 - Formal escalation criteria
- Other Governance
 - Policy Review Committee
 - Change Approval Board
 - Audit Committee



Present Consequences, Not Vulnerabilities



- Risk Domains & Areas
 - Risk Area Assessments
 - Potential for exposure of sensitive information
 - Potential for failure of a legal/regulatory obligation
 - Potential for failure of a key process or service
 - Risk Register
- Findings & Incidents
 - Individual Vulnerabilities
 - Events and Incidents





Program Roadmap

RSACONFERENCE2012

Essential Steps



1. Select a standard/baseline
2. Establish an asset inventory
3. Define your risk scales
4. Profile your environments (sensitivity)
5. Define a workflow for assessing vulnerabilities



Pitfalls to Avoid

1. Don't run a security scan of the entire environment...
2. Don't try to identify and profile every system ...
3. Don't try to build a comprehensive risk model that will account for every possible scenario and special case imaginable...
4. Don't take on large scale assessments until you have proven your methodology ...

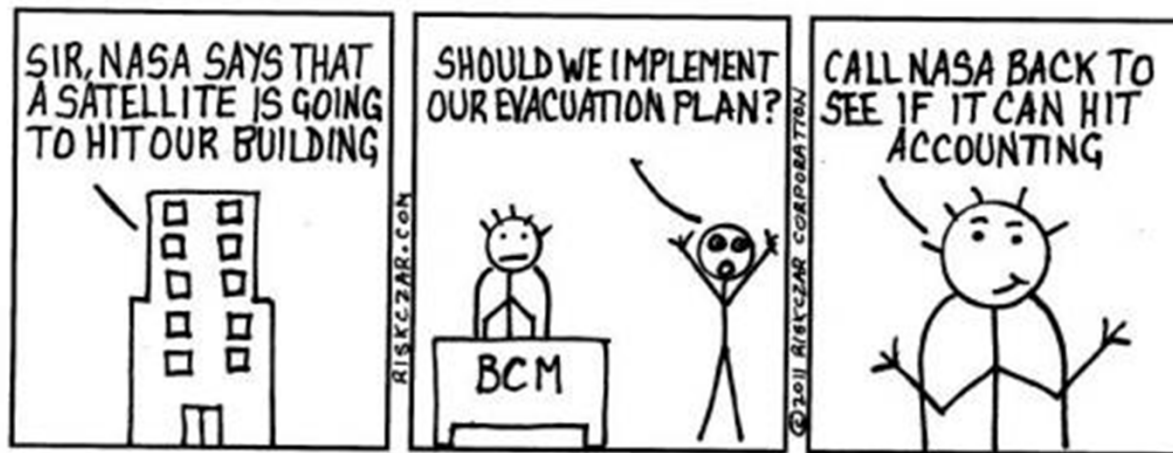


Date		Actions
Year 1	1st Half	<ol style="list-style-type: none"> 1. Develop a plan to address any missing prerequisite items (inventory, policies, etc.) 2. Implement a very basic Threat & Vulnerability Management (TVM) program
	2nd Half	<ol style="list-style-type: none"> 3. Expand your TVM program to highest sensitivity environments and establish measurable metrics 4. Complete Security Risk Profiles for your most critical resources 5. Distribute a Security Risk Review (SRR) questionnaire for just those most critical resources, and focus on qualifying highest risk findings
Year 2	1st Half	<ol style="list-style-type: none"> 6. Refine TVM process and set metrics for all environments 7. Expand the SRR process to include other high sensitivity resources 8. Implement a third-party SRR process with a more targeted list of questions (different from internal questionnaire), and target most critical vendors
	2nd Half	<ol style="list-style-type: none"> 9. Focus on identifying systemic and risk themes from TVM and SRR, and escalate these to senior management
Year 3	1st Half	<ol style="list-style-type: none"> 10. Sponsor an initiative to develop security baselines for critical systems/applications and use these to streamline SRR internally 11. Focus on ways to validate the SRR findings, such as reviewing event logs or scanning results
	2nd Half	<ol style="list-style-type: none"> 12. Document an Enterprise Security Architecture, or at least patterns for well established implementations 13. Identify strong risk indicators, and start tracking them 14. Gather feedback internally about ways to improve the program



Lessons Learned

- Start small
- Start with industry scales and ratings before developing your own
- Focus on oversight, security can't fix everything
- Tie security initiatives to business objectives



Additional Resources



- Security Risk Management: Building an Information Security Risk Management Program from the Ground Up

- ISBN: 9781597496155
- Publisher: Syngress
- Publication Date: May 2011
- Amazon Link: <http://amzn.to/hyrMvC>



- MGT 442: Information Security Risk Management
 - 2 day course
 - Available On Demand & Conference

