



# Global Technology Audit Guide #6:

## Managing and Auditing IT Vulnerabilities



Sasha Romanosky

January 09, 2007

# Outline

- What is The IIA?
- What is a GTAG?
- What does this GTAG Cover?
  - The Vulnerability Management lifecycle
  - Differentiating high and low performing Vulnerability Management organizations
  - Useful metrics to measure progress
- Questions?

# The Institute of Internal Auditors (The IIA)

- International professional organization for IT governance and auditing
- Established in 1941, with 130,000 members from 150 countries
- Provides educational and guidance opportunities and certification programs to IT auditors



# Global Technology Audit Guides (GTAGs)

- Written for the CAE and audit supervisors
- Written in business (not necessarily technology) language – addresses business problems
- Recommend best practices for IT management, IT control and Information Security
- (For this GTAG, we focus on ITIL and larger organizations)

## Previous GTAGs

- Guide 1: Information Technology Controls
- Guide 2: Change and Patch Management Controls
- Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
- Guide 4: Management of IT Auditing
- Guide 5: Managing and Auditing Privacy Risks
- Guide 6: Managing and Auditing IT Vulnerabilities

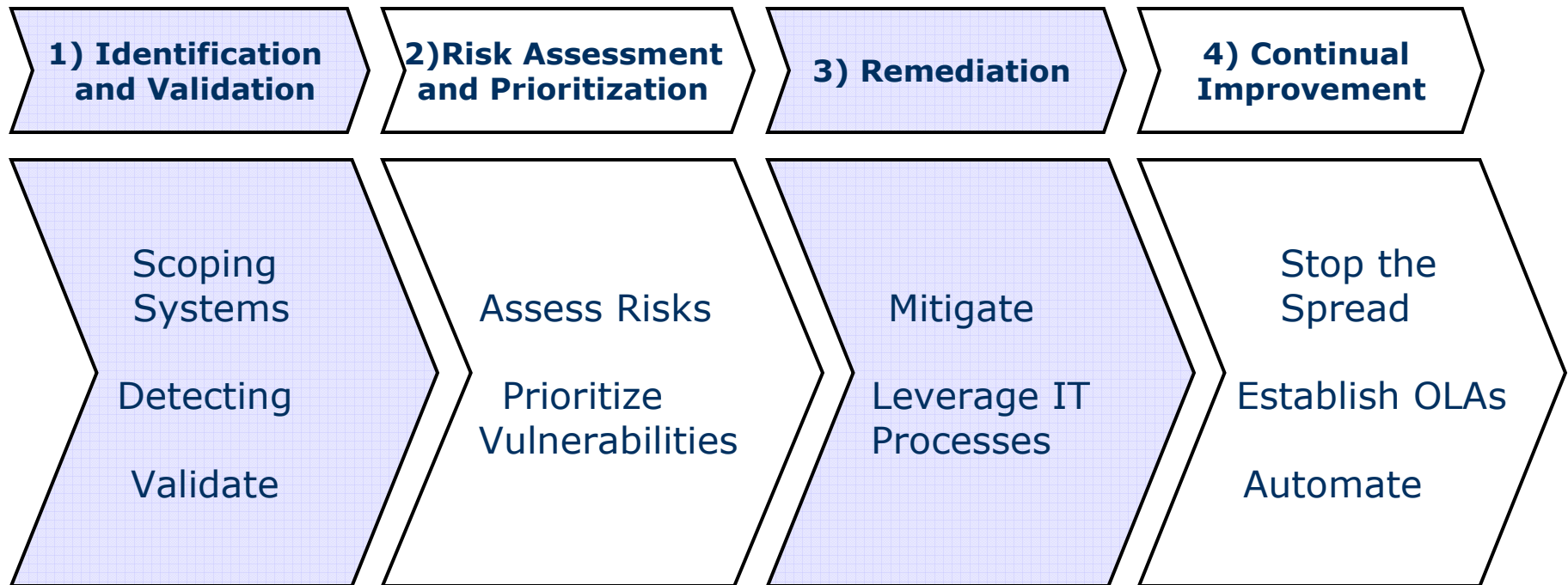
## Previous GTAGs

- Guide 1: Information Technology Controls
- Guide 2: Change and Patch Management Controls
- Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
- Guide 4: Management of IT Auditing
- Guide 5: Managing and Auditing Privacy Risks
- **Guide 6: Managing and Auditing IT Vulnerabilities**

## Why Should You Believe Us?

- Collective experience of me, Bridget (GM audit manager), Gene Kim (CTO, co-founder of Tripwire, and IT Process Institute)
- Gene Kim involved with GAIT project (seeking to differentiate low from high performing IT organizations) – scientific approach
- Leverage proven techniques and processes from ITIL
- Peer reviewed by over a dozens senior IT and audit professionals, including Peter Mell (NIST), Ron Gula (Tenable)

# Vulnerability Management Lifecycle



# Vulnerability Management Lifecycle

## 1) Identification and Validation

- Scoping systems: find all the networks; wireless, backup, transit, admin, test, production. Identify and document them all – even if you won't be scanning them immediately.
- Detecting vulns: all IT assets should be *scanned* or *monitored*, (even printers!) Scanners actively probe devices whereas monitoring passively checks networks or hosts.
- Validating findings: once you have the (mountain of) data, validate the results to weed out false positives

# Vulnerability Management Lifecycle

## 2) Risk Assessment and Prioritization

- Assessing risks: perform a quick risk assessment. E.g.  
Risk = threat likelihood \* vuln severity \* asset value. Take note of security controls that limit or mitigate the actual risk of the vulns.
- Prioritization: prioritize the remaining vulns according to their risk and the effort (cost) required to fix them.
- Also consider how past incidents occurred, this may affect the prioritization. E.g. perhaps all past breaches occurred from 3rd party network connectivity.

# Vulnerability Management Lifecycle

## 3) Remediation

- The challenge is: How to affect change when the motivations of the group finding the vulns aren't (necessarily) those of the group fixing them?
- Leverage (not circumvent) existing IT processes by delivering fixes as just another stock of planned work. For ITIL, this just Change Management.
- IT can then test and coordinate the fixes as necessary. It may not done as fast, but it will get done.
- For most critical vulns: use the emergency change request process

# Vulnerability Management Lifecycle

## 4) Continual Improvement

- Stopping the spread: incorporate changes/patches of current findings into future system builds. (For ITIL, coordinate with Configuration Management.)
- Setting Expectations: By setting proper OLAs, both parties have clear expectations as to what can be done when.
- Automation: much of the efficiency and effectiveness can be achieved through automation of detection, reporting, and remediation (if possible)

# Differentiating Low from High Performers

## 1) Identification and Validation

Low Performer	High Performer
Limited or infrequent detection and scanning of IT systems	Regular vulnerability scans on all 3rd parties, remote offices, VPN clients, corporate and production systems
High variability of IT infrastructure (unmanaged systems), making it difficult to keep track of hosts, networks and system owners	Proper asset management system maintains complete inventory of business owners for all IT assets

# Differentiating Low from High Performers

## 2) Risk Assessment and Prioritization

Low Performer	High Performer
Overwhelmed, possibly paralyzed with volume of vulnerability data	Able to evaluate the cost of remediation and, therefore, better able to prioritize remediation efforts
Unable to assess the risk to IT assets	Incorporates threat, vulnerability severity and asset value to assess risk as best it can

# Differentiating Low from High Performers

## 3) Remediation

Low Performer	High Performer
Inefficient at patching (high variability in patching times)	Reasonable OLAs established with IT management to fix all vulns
Ineffective at achieving fixes from IT management – likely with higher failure rates	Collaborative relationship with IT management and is adept at creating planned work projects

# Differentiating Low from High Performers

## 4) Continual Improvement

Low Performer	High Performer
Few automated processes	Scans are scheduled and reoccurring, the organization is able to track remediation efforts from initiation to fix and report on efficiency
Constantly in a reactive mode when building new systems	Able to cycle back with configuration management to create more secure builds with each scan

# Vulnerability Management Metrics

Metric	Description
Percent of systems scanned	Measures completeness of an organization's VM solution
Number of unique vulnerabilities	Measures the amount of variability -- and therefore -- risk of IT systems
Percent of total systems tracked by Configuration Management	Measures degree to which an organization is aware (and has control) of devices on its network

## Vulnerability Management Metrics (2)

Metric	Description
Percentage of OLAs that have been met	Measures efficiency of the organization's VM efforts
Number of security incidents (per time)	A proxy for effectiveness of the organization's VM efforts
Impact of security incidents	Measures the full cost due to vulnerable systems

# Conclusion

- VM starts by discovery: of networks, devices, and vulnerabilities
- Prioritize according to risk and effort to fix
- Achieve greater success by working with (not against) IT processes
- Establish reasonable OLAs and automate as much as possible



sromanos@cmu.edu