Compliance: How to Manage (Lame) Audit Recommendations

Brian V. Cummings
Tata Consultancy Services Ltd
brian.cummings@tcs.com

Tuesday, August 9, 2011 1:30 p.m.

Session 9221
Security & Compliance Risk Landscape

Presentation addresses the management of Audit recommendations from the perspective of the CISO

Hacking, Phishing, Social Engineering

Sophisticated, automated, stealthy

International and Inter-Enterprise Information Theft

Still acknowledged as the most prevalent and serious threat.

CyberX Activities

X = Crime, Terrorism, Warfare

Legal and regulatory action

Privacy laws, regulations, sanctions, and penalties can jeopardize enterprise viability

Employees

“Loose lips” and careless security behaviors

“Information warfare “ and competition is real and not confined to critical infrastructure.

Sophisticated, automated, and stealthy by organized crime, ad hoc criminals, corporate enterprises, and international intelligence agencies with varying motivations, but all employing highly skilled hackers.
Security & Compliance Risk Landscape

Hacking, Phishing, Social Engineering
Sophisticated, automated, stealthy

International and Inter-Enterprise Information Theft

Internal Fraud and Abuse
Still acknowledged as the most prevalent and serious threat.

CyberX Activities
X = Crime, Terrorism, Warfare

Legal and regulatory action
Privacy laws, regulations, sanctions, and penalties can jeopardize enterprise viability

Employees
“Loose lips” and careless security behaviors

Auditors
Irrelevant, time-diluting recommendations

“Information warfare and competition is real and not confined to critical infrastructure.

Sophisticated, automated, and stealthy by organized crime, ad hoc criminals, corporate enterprises, and international intelligence agencies with varying motivations, but all employing highly skilled hackers.

“Information warfare and competition is real and not confined to critical infrastructure.”
What do you do? What can you do?

If everyone in an entity is not pulling in the same direction, then you won’t get to where you need to be as fast as you need to be there.

Business Alignment
Good Information Security Practices
ISMS Certification
Protection, Enablement, Compliance, Productivity
What do you do? What can you do?

If everyone in an entity is not pulling in the same direction, then you won’t get to where you need to be as fast as you need to be there.

Audit Comment to CISO:
Make sure that all Ethernet ports are disabled if they are not in use to avoid unauthorized intrusion from the Intranet.

Beleaguered CISO
What is wrong with that Audit Recommendation?

• Is it addressed to the person who has the authority to do something about it?
• Is it addressed to the person who can implement and operationalize it?
• What is the real risk relative to other risks the entity may face?
• Is it consistent with the security objectives of the entity and the current plan and budget?
• Is it feasible (solutions, budget, resources)?
What about your Auditor?
What about your Auditor?

- Is your auditor a bully?
- Is your auditor knowledgeable?
- Is your auditor on the right page?
- What is your organization’s attitude toward audit recommendations?
How to manage (all of) your auditors

Take charge and leverage the things you should be doing anyway to help manage your auditors
How to manage (all of) your auditors

- InfoSec Framework
  Set/Lead Program Vision and Strategy
- InfoSec Roadmap
  Set/Lead InfoSec Planning
- Risk Management Program
  Subordinate decisions to a Risk Management process
Information Security Framework

- Business Alignment
- Overall program strategy
- Target Maturity level

- Policy
- Standards
- Procedures
- Automation

- What resources, assets do you have?
- How important are they?
- What are the risks?

- Ownership?
- Funding?
- Implementer?
- Operator?
- Assurer?

Vision

Visibility

Sustainability

Accountability
## InfoSec Roadmap - Strategic

<table>
<thead>
<tr>
<th>Program Domain</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desk Top</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data/Database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environmental</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Multi-Year Planned Milestones**
## InfoSec Roadmap - Strategic

<table>
<thead>
<tr>
<th>Program Domain</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desk Top</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data/Database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environmental</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Or, if you can, plan Q by Q
## InfoSec Roadmap - Tactical

<table>
<thead>
<tr>
<th>Program Domain</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>Governance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desk Top</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data/Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For Current Year, planned and budgeted milestones, allowing for long term projects.
Risk Management Program

- Requirements
  - Business
  - Legal / Contractual
  - Security

- Risk Assessment
  - Asset Identification & Valuation
  - Threat & Vulnerability Assessment

- Selection of Controls (ISO 27001)

- Implementation of Controls

- Information Security Management System (ISMS)
Auditor Buy-In
Auditor Buy-In

First Best Thing To Do

Get Auditor Input and Approval

Second Best Thing To Do

Audit Briefing Paper
Summary: Manage Your Auditors

Establish a collaborative relationship

Leverage your good practices (or establish same)

Communicate frequently
Thank You

Promise what we deliver.
Deliver what we promise. That's certainty.