Introduction

Moderator

Jim Kennedy
Senior Deputy Director of Operations,
State of Ohio

Presenters

Bharath Chari
Cyber Risk Sr. Manager,
Deloitte & Touche LLP

Jeff Goodwin
Advisory Partner,
Deloitte & Touche LLP
Agenda

- Introduction
- System trends
- Compliance and control challenges
- Common security and control requirements
- Project charter and functional requirements
- Risk-based prioritization
- System considerations
- Cloud—Risks and opportunity
- Cloud cyber risk management | Shared responsibility
- Assess cloud cyber risk and assemble a prioritized action plan
- Questions?

System trends

- Cloud based ERP
- Consolidation and replacement of legacy systems
- Automation
- Workflow
- SAAS
- Identity and Access Management
Compliance and control challenges
Numerous regulations, policies and standards may impact a new system and processes automated through it.

Common security and control requirements
At a minimum, existing security and control measures must be maintained during new system implementations. However, opportunities for improvement often exist through newer software features and functionality.

- Address known security and control gaps
- Rationalize security and controls through an updated risk-based approach
- Enhance/strengthen controls through automated/preventative features
- Clean data

• Maintain existing level of controls
• Maintain existing security
• Convert key data
Project charter and functional requirements
Proactive involvement during implementation efforts will help to prioritize and confirm key controls are implemented as required.

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project charter</td>
<td>Streamlined controls</td>
</tr>
<tr>
<td>Functional requirements</td>
<td>Greater automation</td>
</tr>
<tr>
<td>Regulatory and control requirements</td>
<td>Improved governance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Implementation Efforts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess risk</td>
</tr>
</tbody>
</table>

Risk-based prioritization
Proactively map, rationalize and prioritize regulatory and control requirements to achieve a streamlined and effective control model.

**Gather the pieces**
- Identify regulatory and compliance requirements
- Assess risks

**Rationalize and prioritize**
- Sort key regulations and operational requirements
- Find common control requirements
- Prioritize risks

**Achieve long term benefits**
- Compliance and control requirements are met in an efficient and logical fashion
- Future assessment efforts are streamlined
- A consolidated view of all requirements is easily maintained
System considerations
A holistic approach to addressing security and controls based on prioritized risks is beneficial.

Cloud—Risks and opportunity
There are a variety of cyber risks associated with moving to the cloud, yet there are also opportunities.

**Consumer/Shadow IT**
Business and consumers using cloud with or without cyber controls

**Modern attack surface**
The walled enterprise is replaced by a hybrid, more complicated technology environment

**Third-party risk**
Enterprises are dependent on cloud providers’ controls

**Concentrated risk**
Cloud providers are a bigger target because “that’s where the data is”

**Controls gap**
Traditional cyber risk controls need to extend to the cloud at a time when many enterprises are barely keeping up with existing threats
Cloud cyber risk management | Shared responsibility

While cloud providers’ security is often a focus, managing cyber risk is a shared responsibility between the enterprise and the cloud provider.

<table>
<thead>
<tr>
<th>Private cloud (Self-hosted)</th>
<th>Private cloud (Co-located)</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security governance, risk and compliance (GRC)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assess cloud cyber risk and assemble a prioritized action plan

A Cloud Cyber Risk Assessment provides a broad analysis of a client’s current “point in time” state of cyber risks in the cloud and an actionable roadmap to address shortcomings.

- What is my actual cloud service inventory/use?
- Do my existing controls meet industry and organization standards?
- What is my inherent risk?
- What can I do to manage my risks and align to the goals of my business?
Questions?