CYBER RISK MANAGEMENT & THE ROLE OF INTERNAL AUDIT

Catherine Liu, CISA, CISSP, CIPP/US
Disclaimer: The views and opinions expressed in this program are those of the speaker and do not necessarily reflect the views or positions of those of Wells Fargo.
Who am I?

- Sr. Lead Audit Manager, VP @ Wells Fargo
- 15+ years in IT Operations, Risk Management & Control Assurance
- Team Coach, Cheerleader, Change Catalyst, Life-long Learner, National Park Geek, Foodie, Proud Dog Mother
01 Cyber Risk Factors *

* Risk model adapted from KPMG Evaluating cyber risk with internal audits (kpmg.us), 2019
02 Three Lines of Defense (3LOD)

1st Line – Cybersecurity:
- Incident Response
- Security Operations Center
- Automation
- Architecture
- Threat Intelligence

2nd Line – Risk Management:
- Compliance & Governance
- IS Policies
- Application Security
- Risk Measurement
- Third Party Management

3rd Line – IT Audit:
- Assurance Testing
- Independent Risk Assessment
- Consulting Services

Copyright: © Institute of Internal Auditors (IIA) Three Lines Model

The image was adopted from Office of Internal Audit | The Three Lines of Defense – Office of Internal Audit (olemiss.edu)
03 IA’s Role in Cybersecurity

Reference: The critical elements of the IA was adopted from Deloitte POV: Internal Audit 3.0, Modernizing the Three Lines of Defense Model, An internal audit perspective
Copyright: © 2020 Deloitte Development LLC.
04 Examples of Cyber Audit Scope

<table>
<thead>
<tr>
<th>Operations and technology</th>
<th>Information risk management</th>
<th>Human factors</th>
<th>Leadership and governance</th>
<th>Legal and compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability scanning and penetration testing</td>
<td>Vendor risk management and security</td>
<td>IT talent management and training</td>
<td>Cyber governance, roles, and responsibilities</td>
<td>Regulatory considerations and integration into cyber framework</td>
</tr>
<tr>
<td>Network logging and monitoring/threat assessment</td>
<td>Cyber threat analysis and risk management process:</td>
<td></td>
<td>Cyber and enterprise risk management integration</td>
<td></td>
</tr>
<tr>
<td>Device configuration reviews (infrastructure devices, firewalls, routers, etc.)</td>
<td>— Threat identification, assessment, and update process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi – Scanning for unauthorized Wi-Fi/ and Wi-Fi configurations and vulnerability/ exploitation testing</td>
<td>— Including integration with change management and software development lifecycle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote access/VPN points – Technical assessment of the remote access points and configuration to help ensure they are protected</td>
<td>Cloud computer security and ongoing assessment</td>
<td>Data classification, protection, and encryption</td>
<td>Enterprise-wide training and awareness programs</td>
<td></td>
</tr>
<tr>
<td>Application/database assessment – e.g., vulnerability scanning, penetration testing, and DB configuration reviews</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security by design</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architecture reviews and analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system/database security configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patching process/remediation procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code reviews</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Examples of cyber audit scope was provided by KPMG, *The role of internal audit in cyber security readiness.*

Copyright: © 2019 KPMG, LLP
05 Key Cybersecurity Considerations for IA

- Align cyber audit plan to robust frameworks (e.g., ISO, NIST Cybersecurity Framework) to ensure comprehensive domain coverage
- Prioritize risk areas to establish the cyber audit scope; initial assessment can also drive deeper dives later
- Recalibrate cyber audit plan in response to evolving threats, changing regulations, business priorities, and technology adoptions
- Identify talents requirements, relevant experience and skillsets to achieve cyber audit quality
- Evaluate cybersecurity governance risks in context of business goals, strategy, roles and responsibilities
- Monitor the cyber domain maturity (can use Capability Maturity Model Integration/CMMI or other industry recognized maturity models) and evaluate progress against target state
- Report and escalate the risks, timely!
- Use data analytics to drive risk evaluations
- Partner with other lines of defense. Cybersecurity is a team sport
Challenge #1: How to perform an end-to-end audit coverage on cyber risks in a very large organization?

- Case A. Macro-Planning: AgriBank IT Audit Plan Restructuring
- Case B. Process End-to-End: Wells Fargo Application Disaster Recovery Dependency Analysis
- Case C. Horizontal Coordination: Wells Fargo User Access Testing
- Case D. Vertical Deep Dive: Privileged Access

Challenge #2: I don’t know what I don’t know…. How to build oversight over cybersecurity management?

- Case E. Establish Visibility: Measure ICS Policy Adherence

Challenge #3: Busy fighting–fires…. How to prepare the business to survive the next zero–day attack?

Case F. Business Intelligence: Data Driven Audit Procedures
Case G. The Source of Records: Log4J Vulnerability Mitigation
Questions:

What challenges do you see in cyber risk management?

How do you become part of the solution?

I welcome you to share any further thoughts and questions with me!

Catherine Liu
yliu86981@gmail.com
https://www.linkedin.com/in/catherine-liu-72b78a13/

Thank you for your participation!