AUDITING CYBER-SECURITY CONTROLS

Aaron Weller Managing Director, Data Protection & Privacy
PwC

EVOLVING CHALLENGES: EVOLVING PERSPECTIVES

	Historical IT Security Perspectives	Today's Leading Cybersecurity Insights
Scope of the challenge	• Limited to your "four walls" and the extended enterprise	• Spans your interconnected global business ecosystem
Ownership and accountability	• IT led and operated	• Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	• One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain	• Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset protection	• One-size-fits-all approach	• Prioritize and protect your "crown jewels"
Defense posture	• Protect the perimeter; respond *if* attacked	• Plan, monitor, and rapidly respond *when* attacked
Security intelligence and information sharing	• Keep to yourself	• Public/private partnerships; collaboration with industry working groups

QUESTIONS TO ASK & ACTIONS TO TAKE

Question to ask	Actions to take
What data is important?	Understand what data is key across the enterprise and classify it.
Where is it?	Do you control the data, or a third party? Which jurisdiction(s) is it in?
How is it controlled?	What controls have been designed, and are operating to protect key data elements?
How do you know?	What independent assurance do you have that the right controls are working in the right way?

GAINING ASSURANCE OVER CLOUD

Discovery: Where are cloud services being used? A recent study* showed that the average large company has over 700 cloud services in use across their network. The number of these that have been assessed and approved using a formal process? Typically less than 10.

Governance: Governance includes both setting a framework for managing cloud and other third party services, and the ongoing management of that framework to mitigate risk. Effective governance can include:

- Policies
- Vendor risk management
- Contract compliance
- Targeted audits

* SkyhighNetworks Cloud Adoption and Risk Report Q32014

VENDOR ASSURANCE: KEY QUESTIONS

- How do you identify and risk rank your key vendors?
- If you require that vendors protect your data “at least as well as your sensitive data”, how would you go about auditing that?
- If one of your key vendors said that they were “ISO, SOC and PCI Compliant”, what would your next question(s) be?
- How often do you exercise your ‘right to audit’ clause in your contracts?
- If you do exercise your right to audit clause, what do you check for?