APPENDIX

Cloud Computing Audit Checklist

Jeff Fenton

THIS APPENDIX CONTAINS a high-level audit checklist based on selected key points introduced throughout the book. More detail on each aspect here can be found in the corresponding chapters.

Cloud-Based IT Audit Process (Chapter 2)

- ❒ Has the organization applied overall risk management governance to the cloud-provided services? Have relevant risks been identified and treated, including the consideration of insurance where appropriate?
- ❒ Has legal counsel been engaged to evaluate provider contracts and address data protection, confidentiality, and intellectual property issues? Have issues such as source code escrow for provided applications been addressed? What if there is a change in control of the cloud provider?
- ❒ When an existing, internally hosted system is moved to the cloud, have the controls that were provided internally but are not provided in the cloud been identified? When the system was developed internally and is later moved to the cloud, which controls did developers assume or develop that are not provided in the cloud?

Auditing Cloud Computing: A Security and Privacy Guide
by Ben Halpert

- ❒ How will generic patching and testing practices at the cloud provider impact custom systems moved to the cloud?
- ❒ What additional endpoint security measures will be needed once clients access systems in the cloud rather than endpoints behind enterprise gateway controls (firewall, anti-malware, anti-spam, etc.) accessing internal systems?
- ❒ More generally, how are controls being moved closer to the cloud-hosted system and its data because overall controls within an enterprise cannot be applied in the cloud?
- ❒ What identity management, authentication, authorization, and access controls are in place in the cloud, and how will they be audited?
- ❒ How will issues of communication latency, breach notification, and privacy laws/regulations be addressed?
- ❒ Has relevant external guidance been applied (it may include the FedRAMP Program for cloud providers to the U.S. government, European Network and Information Security Agency Risk Assessment, Information Security Audit & Control Association, and the Cloud Security Alliance [CSA] Controls Matrix)?
- ❒ Have core control areas been identified (see Exhibit 2.1)?
- ❒ Have standard audit issues been considered, including auditor independence, auditor technical proficiency and professional practices, and audit reports that clearly present findings and qualified opinions based on evidence?

Cloud-Based IT Governance (Chapter 3)

- ❒ Is an overall information security governance framework in place in the organization? Does the organization understand the criticality of the information it collects, stores, and processes? Are information security investments and program activities aligned with the organization's strategy, risk profile, and business needs? Is there a top-level information security governance committee representing senior management, key business stakeholders, IT management, Audit, and Risk and Compliance to assist the chief information security officer in setting direction for the information security program? Is the information security program's effectiveness regularly reviewed?
- ❒ Does the organization have a written information security policy representing senior management's commitment? Are all personnel required to acknowledge their responsibilities to protect the organization's information resources?

- ❒ Has the organization followed a Governance Implementation and Continuous Improvement Methodology (see Exhibit 3.1) and extended it to governance of cloud computing initiatives?
- ❒ Does the governance committee review service-level agreements for cloud services?

System and Infrastructure Life Cycle Management for the Cloud (Chapter 4)

- ❒ Has the organization identified suitable controls based on mitigating known risks? Is the cost of implementing each control proportional to the cost of exposure? What if the control itself fails? Has the organization anticipated and evaluated unknown risks?
- ❒ Has the organization applied well-known control frameworks (ITIL, COBIT, CSA, NIST) as a starting point?
- ❒ How will the organization verify that controls are in place and operating properly: by direct verification, control attestations, or certification of the cloud provider to standards? Has the organization considered the advantages and disadvantages of a right-to-audit clause?

Cloud-Based IT Service Delivery and Support (Chapter 5)

- ❒ Does the cloud provider offering provide true multitenancy, as distinguished from legacy models such as managed service providers and application service providers?
- ❒ Does the cloud provider offer granular privilege management across all data elements in a multitenant environment?
- ❒ What logging and reporting capabilities does the provider offer?
- ❒ What choices on storage location and encryption does the provider offer?

Protection and Privacy of Information Assets in the Cloud (Chapter 6)

- ❒ Has the organization evaluated the best fit of cloud deployment and service model based on its information protection and privacy needs (see Exhibit 6.6)?
- ❒ Has the organization categorized data according to its sensitivity and the privacy and protection needs associated with levels of sensitivity?

- ❒ Does the organization understand its inventory of data elements based on data producer, data consumer, and sensitivity, along with the life cycle of each?
- ❒ Has the organization assessed the confidentiality, integrity, availability, and accountability needs for each data element at rest and in flight?
- ❒ Has the organization applied this understanding to create a Cloud Information Protection and Privacy Specification (see Exhibit 6.9)?

Business Continuity and Disaster Recovery (Chapter 7)

- ❒ Does the organization have an overall Business Continuity Planning (BCP) program and an IT Disaster Recovery Planning (DRP) program integrated with BCP through supporting the organization's critical business processes?
- ❒ Has the organization considered cloud services to implement or augment traditional DRP activities?
- ❒ Has the organization assessed the BCP and DRP controls at the cloud provider, based on the CSA recommendations?
- ❒ Has the organization considered issues such as retrieving its data in case the cloud provider suffers a disruption, arranging for a backup cloud provider, and verifying that the cloud provider's own DR plan is tested?

Global Regulation and Cloud Computing (Chapter 8)

- ❒ Has the organization identified the laws, regulations, and standards that apply to its business in each country or other jurisdiction in which it operates?
- ❒ Will the cloud provider offer assurances that it can meet regulatory requirements and be audited by the customer organization or a third party for verification of controls?
- ❒ Has the organization involved its audit management function in cloud computing plans from the outset?
- ❒ As part of the service-level agreement, what arrangements are in place for the cloud provider to notify the customer organization in case of a suspected breach? What arrangements for logging and forensic investigation are in place? Would the provider support the investigation?
- ❒ Has the organization considered the geographic location of data stored at cloud providers in terms of privacy and export control regulations? Will the cloud provider guarantee storage of the organization's data in a particular country?

Cloud Morphing: Shaping the Future of Cloud Computing Security and Audit (Chapter 9)

- ❒ Have the organization and the cloud provider considered applying the CSA's CloudAudit initiative?
- ❒ How are security controls such as firewalls, intrusion detection, patch management, and anti-malware granularly applied to virtual environments at the cloud provider?
- ❒ Does the cloud provider associate policy attributes to each data element it stores and apply this metadata approach to facilitate the application of controls? Does each data element generate its own audit trail?
- ❒ Does the customer organization maintain control of encryption keys or use a separate cloud to manage encryption keys?