Evaluating Third Parties Holding Sensitive Organizational Information

Patrick Cunningham, CISM, CIPT, FAI

- Presentation based upon, "Taking the 'Risky' out of Cloud-Based Business", Information Management, January-February 2018

INFORMATION MANAGEMENT
AN ARMA INTERNATIONAL PUBLICATION
JANUARY/FEBRUARY 2018
Volume 52, Issue 1

D DEPARTMENTS
4 IN FOCUS A Message from the Editor
6 UP FRONT News, Trends, and Analysis

F FEATURES
18 **Drawing Ethical Boundaries for Data Analytics**
Jennette Chalcraft, CPA, CA

24 CEO PERSPECTIVE
Principles for Creating a Movement for IG
Jocelyn Gunter, IGP, CPA

28 **Forging a Partnership with IT for Technology Lifecycle Management**
Sue Rock, CRM, and Dennis Trepanier, CRM, CDIA+, PMP

34 FELLOWS FORUM
Taking the 'Risky' out of Cloud-Based Business
Patrick J. Cunningham, CISM, FAI

S 40 MANAGEMENT WISE
Simple Methods for Determining ROI for Records Management Projects
William Saffady, Ph.D., FAI

44 IN REVIEW
Challenging the Archives: A Call to Action for Archivists and Users
Charity Whan

45 IN REVIEW
Navigating the 'New Normal' for Information Careers
Marc Kosciejew, Ph.D.

C CREDITS
48 AD INDEX

What Data?

- What data will be in the hands of the third party?
- Does the data have a data classification?
- Does the data have personally identifiable information, protected health information, or payment card information?
- What is the third party going to do with the information?
- Will the data be accessible from the Internet?
- Are there other regulatory considerations?

Data Flows

- Once you understand the data involved, how will it flow between organizations and users?
  - Is it secured?
- Where will the data will be processed and stored?
  - Is it secured?
- How long will it be retained?
- Services the vendor will provide
- What the vendor will do with the data
- Any subcontractors to be used
- What happens to the data at the end of the contract period?

Key Controls

- Every organization should develop a set of Key Controls that are applied to data both inside and outside the organization.
- For most organizations, this will be around 80 to 100 control statements.
- The control statements will cover areas considered to be important in assessing the risk of a third party

See: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ or https://www.adobe.com/security/compliance.html for some basic controls.

Control Domains

- Asset Management
- Business Continuity
- Backup Management
- Configuration Management
- Change Management
- Data Management
- Identity and Access Management
- Incident Response
- Network Operations
- People Resources
- Risk Management
- System Design Documentation
- Security Governance
- Service Lifecycle
- Systems Monitoring
- Site Operations
- Training and Awareness
- Third Party Management
- Vulnerability Management

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		AICPA 2009 TSC Map	AICPA Trust Service Criteria (SOC 2SM Report)
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer		
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.			X	X	X	X		X	X	X	X		S3.10.0 S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	X	X	X	X	X	X	X	X	X	X	X	X	S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.		X	X	X	X	X		X	X	X	X	X	I3.2.0 I3.3.0 I3.4.0 I3.5.0	(I3.2.0) The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. (I3.3.0) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (I3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies. (I3.5.0) There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.

What is a Control Statement?

- A Control Statement can only be answered yes or no
- Typical control statements might be:
  - [The organization] creates unique identifiers for user accounts and prevents identifier reuse.
  - [Restricted (as defined by the organization's data classification criteria)] data that is transmitted over public networks is encrypted.
  - [The organization] monitors and flags tampering to the audit logging and monitoring tools in the production environment.

Assessing Capabilities

- The typical approach is to send the third party a questionnaire to measure the capability of the third party to meet
- The questionnaire generally includes one line item for every control statement.
- The third party indicates if they comply, and if not, what they do to mitigate the risk, if anything

Evidence

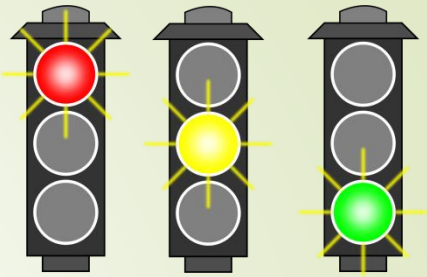
- A major question to be answered by the organization is whether or not evidence will be required for every control
- Evidence will provide a higher level of assurance that the supplier complies with the required controls
- Many suppliers will refuse to provide evidence either because of the workload involved or on grounds of confidentiality
- The organization should keep in mind that evaluating the evidence will increase the assessment time considerably

Assessing Risk

- When the questionnaire is returned by the third party, it should be reviewed
- A scoring mechanism should be developed that accounts for affirmative, negative, and partial answers
  - Each control statement can be weighted by importance
  - A threshold level should be determined that results in an automatic "high risk" rating for the supplier
  - Additional weighting to the scoring can be made for factors relating to likelihood and impact – a higher impact would be associated with more sensitive information; a higher likelihood would often be tied to Internet access

Ideally, automation should be enabled and used as much as possible to speed the assessment – but there may always be some subjective requirements, particularly to assess compensating controls.

Rating Risk



- Keep it simple
  - A "stoplight" rating system should be sufficient
    - Green – no issues of significance
    - Yellow – some issues, but mitigation or compensating controls in place
    - Red – high risk, with insufficient mitigation or compensating controls
- A Red rating should disqualify the third party
- A Yellow rating requires risk acceptance or transfer of risk if mitigation isn't sufficient

Negotiate the Contract

- Once the risk has been evaluated, negotiations with the third party should begin
  - This eliminates wasted effort if the risk rating is High
  - Also eliminates doing business with an unassessed third party
- The contract should include an appendix that includes, verbatim, the same set of controls that were assessed
- Ensure the Controller and Processor are defined
  - And what limitations on use or sharing are in place
- Cycle time becomes an issue, especially in environments where agility is demanded

Ongoing Monitoring

- A provision in the contract should allow recurring and ongoing monitoring of the third party against the controls
- On a periodic basis, the third party should be sent a questionnaire to determine if the controls are being met or if any changes have taken place
- In certain instances, a formal, often on-site, audit of the third party's practices may be warranted
  - This must be specified in the contract

A Comprehensive Qualification and Assessment Cycle

- Supplier Selection
- Supplier Qualification (D&B review, fitness to task)
- InfoSec Assessment
- Other Regulatory Assessments (Privacy, GxP, etc.)
- Risk / Mitigation Review (Accept, Avoid, Mitigate, Transfer)
- Supplier Down Selection
- Contractual and Pricing Negotiations
- Contract Execution
- Monitoring
- Ongoing Risk / Mitigation Review

Alternatives

- Some third parties may prefer to provide a standardized response.
  - The organization should determine
    - If ISO 27001 certification is sufficient
    - If a SOC 2, Type 2 report is sufficient
      - (unless the third party is integrated into the organization's financial controls, a SOC 1 is generally insufficient relative to security controls)
- An emerging trend is Shared Assessments / Standardized Control Assessments
  - An independent organization conducts a standardized assessment (on a regular basis) of a supplier organization; potential business partners can purchase or subscribe to the assessment.
  - Reduces supplier and purchaser workload; creates more level playing field
    - Challenge: Unique or industry-specific requirements

Shared / Standardized Control Assessments

- VSAQ (Vendor Security Assessment Questionnaire) – Google (https://opensource.google.com/projects/vsaq)
- SIG and SIG Lite (Standardized Information Gathering) – Shared Assessments Program (https://sharedassessments.org/)
- CAIQ (Consensus Assessments Initiative Questionnaire) – Cloud Security Alliance (https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/)