BUSINESS-TECHNOLOGY GUIDANCE

ASSOCIATES, LLC.

Building Security Into Contractual Agreements: Bid Specifications, SLAs and MOUs

Tuesday, September 20, 2016 –

FAEDS 2016

Agenda

In this webinar we will explore some of the security related considerations that should be written into Service Level Agreements and Memorandum's of Understanding. During the morning we will talk about:

- How regulations and industry requirements regarding data security and privacy are changing the way contractual arrangements are documented
- The need for introducing security related concepts at the RFP stage
- The need for data related receptacle agreements
- How data ownership and custody should be declared and documented in a SLA or MOU
- Sources to aid organizations in building contractual documentation from Educause and others

At the end of today's session you should have a better understanding of how to build security into contractual agreements and some of the items to look for to assure effectiveness of these agreements.

Why Outsourcing is Gaining Popularity

EXAMINING THE CHANGING IT LANDSCAPE

Environments

- Companies may elect to outsource (in part or completely) their:
  - Infrastructure
  - Services
  - Applications
- Outsourcing can be domestic or overseas “Offshoring” as well as when a company uses another of its subsidiaries/divisions.

Roles and Responsibilities

- Service Provider
  - Accountable for ensuring adequate data protections based on data classification
- Client Enterprise
  - Ultimate Accountability for Reputational and Legal Risks

Why Data Classification Matters In The Selection Process

DATA CONSIDERATIONS

Information Asset Inventory

- Information Asset Inventory
  - Asset Name
  - Asset Description
  - Data Classification (and required treatments)
  - Record Retention Requirements
  - Record Destruction Requirements
  - Asset Location
    - Path
    - In-house or vendor

Information Asset Inventory

- Information Asset Inventory
  - Asset Owner
  - Asset Cross Reference to Associated Controls
  - Asset Cross Reference to Legal and Regulatory Requirements
  - Asset Cross Reference to Business Process
  - Asset Cross Reference to Enterprise Objective
  - Assets Cross Reference to Associated Vulnerabilities, Threats and Risks

Contracts Should Articulate Data Ownership / Custodianship

REGULATORY/INDUSTRY CONSIDERATIONS

Regulation Overview

- Regulations regarding any data the service provider might collect, store and process on behalf of the enterprise.
- Executed Contracts and Service Level Agreements articulation of the state, national or international laws applicable to ensure legal compliance.
- The next several slides discuss where SLA and MOU requirements are being integrated into various regulations

FERPA

- FERPA requires that institutions protect the privacy of student education records in their possession as well as provide the student (or parents/guardians for students under 18) access to such education records.
- Agreements include contract language that clarifies the institution retains ownership of any education records maintained by Cloud Provider
- Agreements include contract language that clarifies the education records will only be used as directed by the institution or the student via a signed consent
- Agreements include contract language that clarifies the education records will be destroyed or returned to the institution if the contract is ended at the discretion of the institution

FERPA

- Physical protection of education records it creates and maintains for the postsecondary institution by storing those records on its own exchange server system
- Appropriate procedures are in place to control access and maintain security of records
- Records will be stored on servers an encrypted format with name and password protection
- Institutions have the ability to allow student access to education records upon request of the student
- All requests to education record access by students are directed to and controlled by the institution

COPPA

- Strict parental notice and consent requirements “on operators of websites or online services directed to children under 13 years of age
- collection of children’s data “is limited to the educational context—where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose.”

COPPA

- formal processes at the institution level for assessing vendors’ privacy practices
- *schools or school districts* decide whether a particular site’s or service’s information practices are appropriate
- Institutional accountability for privacy of student information
- requires website and online service operators to obtain “verifiable parental consent,”

COPPA

- personal information - name and address, screen names, geolocation data, and persistent identifiers
- A persistent identifier is a way to cross reference a user across websites. IP addresses, MAC addresses and even cookies

*This is why Secure Coding and the OWASP Top 10 is so important!

PPRA

Protection of Pupil Rights Amendment

It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

- political affiliations or beliefs of the student or the student’s parent;
- mental or psychological problems of the student or the student’s family;
- sex behavior or attitudes;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;

PPRA

It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

- legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- religious practices, affiliations, or beliefs of the student or student's parent; or,
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

*This is where we build rules into the systems to reduce the likelihood of non-compliance

PCI 3.2 – REQ. 12.8.2 and 12.9

- Receptacle Agreements Regarding Data Related Responsibilities
- Statement of Work and Service Level Agreements should stipulate the exact procedures in place for data handling at rest, in transit and during processing
- Learn more at: www.pcisecuritystandards.org/documents/PCI_DSS_v3.2.pdf

FedRAMP CONOPS

- SLA and MOU *Template Requirements from PMO*
  - *http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf*

FISMA – What's Ahead?

- "**Review of Security in Contract Clauses:** As a result of cyber incidents impacting Government information that resides on or is connected to contractor systems, a group of experts in security, privacy, and the Federal acquisition process were tasked with reviewing existing contract clauses and providing recommendations to improve cybersecurity protections in Federal acquisitions. The group's recommendations were used to inform the development of OMB guidance, titled *Improving Security Protections in Federal Acquisitions*. The guidance, to be released in the first quarter of FY 2016, provides clarity around requirements for security in Federal acquisitions. " Learn more at the link below!
  - https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

Reality Check

- **"5.1.15 For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems. "**
- Search SLA to learn more at:
  - http://www.usda.gov/oig/webdocs/50501-0008-12.pdf

Knowing the Inherent Risk of Outsourcing

THIRD PARTY RISK

Risk Considerations

- Vulnerabilities to consider when assessing risk related to 3rd Parties include:
  - All Access Points
    - If it has an IP address and connects to your network it must have unnecessary communications ports and services disabled. If enabled, strong passwords and adequate encryption, logging and monitoring are musts.
  - Cross contamination of records amongst completers (access issues)

Risk Considerations

- These risks fall into the following categories and need to be considered when selecting a vendor to safeguard your data/information:
  - Financial Loss
  - Reputational Damage
  - Legal Sanctions and Regulatory Fines and Penalties
  - Cyber
  - Geopolitical
  - Terrorism

Risk Considerations

- These risks fall into the following categories and need to be considered when selecting a vendor to safeguard your data/information:
  - Bribery
  - Fraud
  - Organized Crime
  - Hack Activist

Selecting the Right Solution Through Research and Assessment

THE RFP PROCESS

The RPF Process

- The Request for proposal is the opportunity to open the intent to purchase up to a group of providers
- The details placed within the RFP not only inform the potential client of the offerings of the vendor but also lay a groundwork for the long term relationship of the selected partner

Non-disclosure & Receptacle Agreements

- Two important documents to accompany the RFP are the Non-disclosure agreement and the Receptacle Agreement

Non-disclosure Agreement

- The Non-disclosure is needed if you are going to share Intellectual Property and/or Customer or Proprietary Data and Information
- The agreement should state:
  - What data and information is going to be provided, how, by whom and when
  - How the data and information can be used (and by whom) and how it must be stored, transmitted and destroyed

Receptacle Agreement

- The Receptacle Agreement draft should also be provided upfront so you are in command of defining the roles and responsibilities of the data owner and data custodian should the relationship transpire
  - The Receptacle agreement should:
    - Be very detailed covering data and information (as separate topics) from inception to destruction
    - Describe the roles of each party and how data and information should be protected throughout it’s life cycle

Preparing the RPF

- Before an effective RFP can be developed certain activities should take place including:
  - Identifying all stakeholders
  - Gathering and formalizing business requirements
  - Gathering and formalizing functional requirements
  - Mapping the current business process
  - Mapping the current network
  - Mapping current data flow
  - Listing of Regulations and required controls

Preparing the RFP

- The following policies should be gathered and reviewed so their principles are incorporated into the RPF process:
  - Information Security
  - Access
  - Encryption
  - Data Classification
  - Record Retention
  - Other applicable policies that will apply to the proposed solution

Preparing for the RFP

- Details described should now be fed into the RPF in the form of compatibility questions
- RPF should be sent to multiple viable vendors as not all may reply or be fits once culture, policy, regulation and conformance to business requirements are assessed

Assessing the Result

- Review assessment results two-fold:
  - First, create a scorecard with a scale for each question and criteria for each grade. Review the vendors answer and score their answer. The three vendors with the top scores then go into round 2
  - Second, schedule each of the finalists to provide a demo and participate in an architectural review / risk assessment exercise

Due Care

- Perform a Due Care Review on the finalist to ensure they meets financial, cultural and security considerations

Ensuring Data is Protected

DATA RELATED RECEPTACLE AGREEMENTS AND S.O.W.

General Content

- The reciprocal agreement should contain:
  - Background regarding the relationship between the entities engaged in the agreement
  - What information is to be shared between the entities (and to any additional entities)
  - How the information will be stored, transmitted and processed including the tools to be used
  - Nice Example https://solanabeach.govoffice3.com/vertical/Sites/%7B840804C2-F869-4904-9AE3-720581350CE7%7D/uploads/Item_A.3._Report_(click_here)(2).pdf

General Content

- The SOW (Statement of Work) will compliment the Reciprocal agreement by describing:
  - What data is to be exchanged and for what purpose
  - Legal and Confidentiality Provisions
  - Bullets articulating the specific responsibilities of each party
  - Specific terms and conditions and their definitions
  - Data Layouts for both entities
  - Confidentiality Statements (for both parties to sign)
  - https://solanabeach.govoffice3.com/vertical/Sites/%7B840804C2-F869-4904-9AE3-720581350CE7%7D/uploads/Item_A.3._Report_(click_here)(2).pdf (Nice Example)

How data ownership and custody should be declared and documented

SLA OR MOU

SLA

- The SLA should be an extension of the Contract. It provides additional detail regarding the specific services provided along with criteria where the provider may either receive a bonus or penalty where the agreement criteria is violated
- Organizations use the SLA as a tool to manage the provider’s degree of compliance with the contract
- SLA are considered agreements between two parties and contain an offer and acceptance which can be enforced in a court of law

SLA Basics

- The SLA will generally contain the following data:
  - Agreement Overview
  - Purpose, Goals and Objectives
    - The **purpose** of this Agreement is to …
    - The **goal** of this Agreement is …
    - The **objectives** of this Agreement are to:
      - Provide clear reference to service ownership, accountability, roles and/or responsibilities.
      - Present a clear, concise and measurable description of service provision to the customer.
      - Match perceptions of expected service provision with actual service support & delivery.
  - Stakeholders (Description)
  - Periodic Review (includes effective dates, roles, activities and timing)

SLA Basics

- The SLA will generally contain the following data:
  - Service Agreement
    - Service Scope (Services Covered)
      - CIA
      - Change Control
      - Business Resiliency
      - Help Desk Support
      - Contractual Compliance Validations
    - Customer Requirements
    - Service Provider Requirements
    - Service Assumptions

SLA Basics

- The SLA will generally contain the following data:
  - Service Management
    - Service Availability (Coverage)
    - Service Requests
    - Incident / Problem Reporting
    - Training Requests
    - Reporting Requests
    - Assurance Requests

Service Level Agreement (SLA)

- FedRAMP & NIST 800-53R4
- MITRE 2015 Update – See Chapter 7 – SLA and throughout document for various Security Considerations:
  - https://www.mitre.org/sites/default/files/publications/pr_15-2504.pdf
- Europe Example: http://easa.europa.eu/essi/ecast/wp-content/uploads/2015/09/EOFDM_WGC_MoU_15.Sept_FINAL.pdf

SLA

- Another Excellent Source:
  - https://www.sans.org/reading-room/whitepapers/cloud/proposal-standard-cloud-computing-security-slas-key-metrics-safeguarding-confidential-dat-35872

MOU

- A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.
- It generally defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
- It describes the terms of an arrangement between parties and includes offer, acceptance, intention and consideration but generally cannot be enforced in the court of law and is only binding if signed in exchange for $

MOU Basics

- **Memorandum of Understanding**
- Between (Partner) and (Partner)
- This Memorandum of Understanding (MOU) sets for the terms and understanding between the (partner) and the (partner) to (insert activity).
- **Background** (Why partnership important)
- **Purpose** This MOU will (purpose/goals of partnership)
- **Goals** The above goals will be accomplished by undertaking the following activities: (List and describe the activities that are planned for the partnership and who will do what)

MOU Basics

- **Reporting** (Record who will evaluate effectiveness and adherence to the agreement and when evaluation will happen)
- **Funding** (Specify that this MOU is not a commitment of funds)
- **Duration** This MOU shall become effective upon signature and will remain in effect until modified or terminated by any one of the partners by mutual consent. In the absence of mutual agreement by the authorized officials from (list partners) this MOU shall end on (end date of partnership).
- **Contact Information** (FOR ALL PARTIES)
- **Signatures with Dates**

Memorandum of Understanding (MOU)

- Examples:
  - https://aait.ucsb.edu/projects/data.management.system/DMS.MOU.UCSB.UCI.2015.16.pdf
  - 800-47 Appendix B: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

Interconnected Security Agreement (ISA)

- The ISA details the “interconnection arrangement” between two entities (companies)
- It describes in detail, what is required in order to provide overall security safeguards for the systems being interconnected.
- The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
- An example can be found in 800-47 Appendix A: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

ISA Basics

- Overview describing the need to interconnect two systems including how CIA is ensured
- System Security Considerations including details about the data and its environment and protections
- Network and Data Flow Diagrams along with detailed descriptions
- Software description including configuration descriptions
- Roles and Responsibilities
- Schedule for completion and compliance checking
- Security including Access / Roles
- Mapping to NIST 800-47
- Signatures between parties

Contract Related Aspects Regarding Security

NIST CONNECTION

MOU & ISA

- NIST 800-47 assists entities with developing a baseline for achieving information security. Within the document it describes the roles of the MOU and ISA
- It is recommended that a Implementation Plan be documented that includes a detailed description security controls, hardware – topology diagram and software – services/apps; Data Flow diagram; Roles and Responsibilities including various tasks and procedures including risk assessments and re-certifications; operational and security testing; user awareness training; schedule, budget, documentation.
- See appendix C 800-47 and 800-27A

Due Care

ASSURANCE CONSIDERATIONS

Assurance Basics

- Assurance activities are designed to measure the reasonable effectiveness of controls
- Audit Risk: “That controls are not effective and will not be identified within the assurance engagement” *is a big concern as these assessors require greater knowledge of technology then traditional IT control assessors*
- The Extended Enterprise – Everything as a service; Outsourcing; Offshoring

Step 1

Before reviewing the vendor’s side… start by assuring the reasonable effectiveness of your internal vendor management processes!

- Review Vendor Management Governance
  - Ensure there is adequate oversight and controls in place including a comprehensive set of Vendor Management related policies and procedures
  - Validate the adoption and adherence to industry accepted standards for vendor engagement, evaluation and approval/rejection (for both new and existing vendors)

Step 2

Review the Due Care Procedures and Test for Compliance (New Contracts, Annually and During Contract Renewals). Specifically look for the evidence that the following items are being assessed:

- Financial Review
- Onboarding Process
- Information Security Policy
- Business Continuity / Disaster Recovery Policy
- Record Retention Policy
- Record Destruction Policy
- Affiliates / Third Parties Used
- Self Assessments, SSAE 16 SOC 2 Type 2, ROC, etc.

Step 3

Review a sample of the contracts for conformance with policy and regulations:

- Ensure all contracts with outside entities that store, process or transmit data that has a regulatory or legal implication have specifically stated contract provisions regarding:
  - responsibility for protecting data based (plus reciprocal agreement) on applicable laws and regulations
  - the necessity for the vendor to comply with privacy and information assurance policies and practices for of the enterprise.
  - Adequacy of vendors Risk Management, Incident Response, Information Security, Business Continuity and Business Continuity and Vendor Management Programs

Assessing the Due Care Process

- During an IT Outsourced Environment Review the assessor should focus attention on the following areas:
  - Ensure each contract explicitly articulates not only the right to audit but also where there is the expectation to comply internal policies and practices regarding but not limited to Information Security, Data Governance and Management, System Monitoring, Architecture, Change Control, Project Management Supply Chain
  - Verification that the documented business requirements continue to be achieved
  - Ensuring continued compliance with contract and treatment for exceptions

Assessing the Due Care Process

- During an IT Outsourced Environment Review the assessor should focus attention on the following areas:
  - Reviewing the Relationship Management activities – verifying continued independence and touch points with competitors
  - Assessing the effectiveness of the functionality and controls under the control of the vendor(This is accomplished through direct audits, questionnaire's or through work of others – SSAE 16 Type 2 SOC 2, PCI ROC, etc.)

Assessing the Due Care Process

- During an IT Outsourced Environment Review the assessor should focus attention on the following areas:
  - For SSAE16 – Ensure all Client Considerations are addressed internally as well as any assessor finds that conflict with your companies policies and procedures
  - Validating fulfillment of assurance charter and compliance requirements for the data assets held/used by the outsource

Assessing the InfoSec Components

- Topics to be incorporated in our engagements around Information Security include:
  - Data Classification
  - Asset Inventory
  - Configuration Management
  - Data Management
  - Access Management
  - Data Privacy Management
  - Awareness Training

Assessing the InfoSec Components

- Topics to be incorporated in our engagements around Information Security include:
  - Change Management
  - Problem Management
  - Incident Management
  - Vulnerability Assessments
  - Business Continuity / Disaster Recovery
  - Encryption / Key Management

Tips

- Starting with the Charter, look for evidence of signoff and support from governance bodies
- Ensure policies are supported by a set of procedures and are measured by a industry recognized set of standards
- Ensure all policies compliment one another to provide protection of data throughout its life
- Ensure the Data Classification Policy identifies all types of data and that there are clear treatment descriptions and cross references to other policies which support including SDLC, Security Coding, Access, Retention and Disposal
- Focus on CIA
- Don’t forget about 3rd parties

Tips

- Develop Substantive tests for the topics discussed in the last two slides
- Gather and assess along with policies and procedures: Data Flow, Network and Process Diagrams as well as results from Penetration Tests, Vulnerability Assessments, Patch Management, BCP/DR Exercises, Incident Response Exercises, Problem, Change and Incident Tickets, Project Risk and Issues Logs, Past Audit Results and Security Exceptions
- Ensure physical and logical access are assessed too

When is enough, enough

BUT THEY SIGNED THE AGREEMENT

Control Validation

- So we have an agreement signed by all impacted parties before we give computing devices to students and we retain those documents for a period of time. Why would that possibly not be good enough?

Control Validation

- Controls need to be SMART!
- Compliance Test
  - Validate there is a signed agreement between parent and institution
- Substantive Test
  - Ensure awareness training for students by grade, parents and educators at least annually
  - Ensure logging in place to capture activities and exception reports are created to notify both violations and successfully completed tasks

Questions to Accompany Every Technology Spend Decision… and how knowing the answers to theses can aide in future audits

TOP 10 QUESTIONS

#1 – Data Management

- Explain Data Management Process
  - Does the solution utilize the 2016-2017 FL Educational Data Dictionary? If yes, is it updated annually?
  - Has a legal agreement been created with the vendor acknowledging there willingness to abide by the institutions Data Classification and Data Privacy Policies?
  - Has the institution provided the vendor with required control objectives and test scripts?

#1 – Data Management

- Have the vendor provided copies of backup policies to ensure OS, Application, Configuration and Data are backed up in accordance to institutions requirements are being retained for the correct period?
- Has the institution validated data (and database) restore procedures exist and are tested at least quarterly?
- Is the data available for End User Solutions and if so, have the “opt out” records been excluded?

#1 - Data Management

- Have the vendor provided detailed restore procedures?
- Has the vendor provided a data flow diagram?
- Has the vendor provided a scrubbed network diagram?
- Has the vendor provided a system /process (module) flow diagram?
- Have the vendor provided proof of date destruction and provided their process?

#2 – Information Management

- Explain Information Management Process
  - Are FERPA and COPPA reporting requirements built into the solution?
  - Have the institution provided the vendor with their Record Retention Policy?
  - Have the institution validated the backup policy is in place to ensure the information (reports) are being backed up and saved for the correct period

#2 – Information Management

- Has the institution validated information restore procedures exist and are tested at least quarterly?
- Have the vendor provided proof of date destruction and provided their process?
- Is the information available for End User Solutions and if so, have the “opt out” records been excluded?

#3 – Log Administration

- Explain Log Administration Process
  - What data is written to log files?
  - Is restricted and non-restricted personally identifiable student as well as standard PII, PHI and PAN data encrypted according to the clients shared Data Classification Policy?
  - Is information captured in logs in accordance to the Institutions Data Privacy and Record Retention Policies? (Do not forget about Opt Out Provision)

#3 – Log Administration

- Is information captured in logs available on-demand to the institution?
- Can the logs be extracted into the institution log correlation and security analysis engine?
- Have the business requirement and functional Use & Misuse Cases been incorporated into the vendors analytics engines so abnormal actions / conditions are quickly identified and reported? (IDP, IPS, SEIM, DLP, LDAP, SA, etc.)

#4 – Access Administration

- Explain User Provisioning
  - How is access approved? Granted? Entitled?
  - Who has capability to grant/alter access?
  - Can ID’s be deleted without harming log files or must I retain id’s in a inactive state indefinitely to retain accuracy on activity related reporting?
  - How are privileged rights administered?
  - How are privileged rights monitored?

#4 – Access Administration

- Does the vendor solution allow for IAAA (Identification, Authentication, Authorization and Auditing)
- Does the solution allow for role administration? Can an ID be assigned to multiple ID's (SOD)?
- What alerting capabilities exist? HIDS, HIPS, HDLP

#5 – Certification and Accreditation

- Explain Go Live and Updates
  - Do the hardware and software components go through both a offline sandbox vulnerability scan and final accreditation before go live and for each update there after?
  - Does the vendors patch management process align to the institutions?

#5 – Certification and Accreditation

- Does the vendors vulnerability scanning process align to the institutions?
- Does the vendors penetration test schedule and depth align with that of the institution and the regulations they abide too?

#6 – Services Management

- Do patches and configuration changes (firewall, router, application, etc.) all require change tickets?
- Does the vendor have a formal change control process and is the institution alerted prior to change implementation?
- Does the institution have a complete Asset Inventory including all Information Assets?

#7 – Risk Management

- Does the contract contain provisions for the vendor to be engaged in the institutions annual information security risk assessment? (What is vendors role and what must they provide?)
- Are the results of the assessment incorporated into the institutions risk register (and tracked for remediation status) and risk profile calculation?

#8 – Vendor Management

- Did the institution review the vendors SSAE16 SOC2 TYPE 2 and map all “Client Considerations” to internal controls?
- Did the institution include a “right to review vendor onboarding and renewal process” in the vendor’s contract?
- Was and adequate level of due care conducted before contract signing? Reviewed?

#9 – Incident Management

- Was the AIW established?
- Does the vendor have a well documented and complete Incident Response Plan?
- Does the institution participate in annual Incident Round Table exercises?
- Does the institution have a clause in the SLA for time to notify if its data is exposed while in the vendors possession? Are event communication intervals established? DR Declaration requirements? Event reporting?

#9 – Incident Management

- Has the institution provided requirements with the vendor for documenting actual events in accordance with regulatory reporting requirements?

#10 – Business Resiliency

- Did the Institution participate in a Business Impact Assessment with the Vendor during design and annually or as changes were needed there after?
- Are Business Continuity and Disaster Recovery plans established by the vendor for the institution? Did institution approve plan?
- Were the RTO/RPO baked into the solution?

#10 – Business Resiliency

- Does the institution participate in annual BCP and DR Drills?
- Has the institution provided requirements with the vendor for documenting actual events in accordance with regulatory reporting requirements?

Let’s Talk About LMS Consideration

YOUR TURN – OPTIONAL EXERCISES

Exercise 1

- You and your team have been tasked to research a new LMS.
- The stakeholders include teachers, parents, administrators and students
- The major business requirements for the new solution include:
- Ability to allow student to student and student to teacher collaboration; ability to share assignments and results between parent, teacher and student; ability to create and modify course content without knowledge of scripting languages

Exercise 1

- With your team, review the sample RFP form and discuss the forms content and what you would want to make sure to include and what you would be looking for as results.
- Take 20 minutes and prepare a 5 minute overview for the group

Exercise 2

- The RFP process is complete and we are ready for the Due Care Process.
- As teams discuss the Checklist and how you and your team would go about accomplishing the items including items you might exclude and/or other items you might include
- Take 20 minutes and prepare a 5 minute overview for the group

Wrap-up

- Planning is the basis of a success implementation and that process starts before the RFP “Bid” is developed
- Having a standardized onboarding process from RFP to Architecture Review, to Risk Assessment & Due Care Review is necessary
- Once onboard, assessing the effectiveness of the solution is needed to better ensure effective data governance and management

Sources for More Details

- Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing.”
- ISACA Outsource Audit and Assurance Program
  - http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx
- SANS on Outsourcer Audits
  - https://www.sans.org/reading-room/whitepapers/auditing/outsourced-information-technology-environment-audit-33338
- Auditing Big Data
  - http://www.journalofaccountancy.com/news/2014/oct/201411104.html
- http://familypolicy.ed.gov/ppra

Sources for More Details

- https://iapp.org/news/a/coppa-in-the-classroom/
- http://www.lhcss.org/legislative/cloudcomputing-privacy.pdf
- http://olc.onlinelearningconsortium.org/effective_practices/adhering-ferpa-while-computing-cloud-and-proctoring-exams-online
- http://www.marketwired.com/press-release/ferpa-update-could-extend-to-third-parties-2013336.htm

Sources for More Details

- https://cdn-files.nsba.org/s3fs-public/01-Myers-2016-FERPA-Update-Paper.pdf
- http://blogs.edweek.org/edweek/DigitalEducation/2015/04/ferpa_overhaul_US_House.html
- https://epic.org/apa/ferpa/FERPA-discussion-draft.pdf
- http://www.securityprivacyandthelaw.com/2016/02/ftc-announces-coppa-settlements-based-on-persistent-identifiers/

Sources for More Details

- https://cdn-files.nsba.org/s3fs-public/01-Myers-2016-FERPA-Update-Paper.pdf
- International Privacy related topics
  - http://blogs.dlapiper.com/privacymatters/
  - http://www.dlapiperdataprotection.com/#handbook/law-section/c1_BR
  - http://www.publicit.co.uk/2014/02/new-in-iso270012013-secure-systems-engineering-principles/
- http://www.ready.gov/sites/default/files/documents/files/IS_system_development_cycle.pdf (Share with your Security and Development Teams)
- http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Thank you!

If you would like additional information regarding any of today's discussing please contact me by email, Google+, LinkedIn, Twitter, Facebook or Phone:

Shawna M Flanders CRISC, CISM, CISA, CSSGB, SSBB

Business – Technology Guidance Associates, LLC.

sflanders@bustechga.com

www.bustechga.com

https://www.linkedin.com/in/sflanders

https://www.facebook.com/Business-Technology-Guidance-Associates-LLC-544587322229503/?ref=hl

www.twitter.com/shawna4training

https://plus.google.com/110253813467082085462

727-491-7337 or 844-4BUSTECH (Office)

727-483-3662 (Mobile)

941-621-4980 (Fax)