Changes in the Checklist for 11. Information Technology

I am glad that the checklist has been updated to include more recent technology. Updating the checklist was a step closer to closing the gap between the business and technical side of systems. I look forward to the future use of the checklist. – Brittany Lennon

General Changes

- EDP changed to IT
- Original Checklist contained 5 sections along with an additional checklist.
- Updated Checklist contains 6 sections.
- Updated Checklist contains updated language for objectives in each section. The updated language condenses the objectives to their main ideas, instead of multiple points hit.
- Subsection added to E. Specific Application
    - Subsection added for Remote Work.

Changes in Objectives

A) Objective bullet list was simplified to "Ensure the entity establishes effective Information Technology (IT) governance over its information technology and data" which incorporates the intentions of the former list.
   i) Although word choices were changed and updated to fit the current IT standards and technology, the spirit of all original controls are still present
   ii) Combined policy and procedure controls into one control using "including but not limited to"
      1) Idea behind this is so it can be a minimum list of policy and procedures. This allows agencies discretion to add on to the list to tailor to their needs.
   iii) Controls will now reflect the current IT environments, including 3ed parties & the request for SOC reports(expanded upon), a remote work policy, and additional content for backups such as restore and retention.

B) Objective focuses on data loss prevention.
   i) More controls aimed at backups and ensuring there are: procedures in place for backups including hosting environments, verification of backup, testing of backups, encrypting sensitive information, etc.
   ii) Expanded Disaster Recovery control
   iii) Logging and monitoring functions expanded in controls

C) Objective includes proactive and reactive physical and logical access prevention.
   i) Expanded access right controls
   ii) Expanded vulnerability mediation
   iii) Updated backup controls
   iv) Expanded on logging and monitoring
   v) Physical security expanded upon

D) Objective is meant for all new system development or system modifications.
   i) Emergency change controls expanded
   ii) Additional "system methodology includes" added:
      1) Reason for change
      2) Key performance measures
   iii) Internal Audit group review changed to pre-implementation review
E) Objective is meant for all current systems in use.
   i) Added language as to what system to review was added
      1) I.e. Critical function implications
      2) Financial reporting implications
   ii) Added subsection: Controls applicable to the hosting environment
      1) These controls are only solutions with a hosting environment

F) Objective is for remote work controls
   i) Includes:
      1) General policies
      2) Security of data and network
      3) Inventory of: equipment & those with sensitive data access

Problem Controls:

- Objective A:
  - The first objective is about the governance over IT. Governance cannot be performed without set policies and procedures, defined responsibilities and expectations, without goals and evaluations. First come policies and procedures; many agencies struggle with that as it is time consuming and monotonous process. Unfortunately, it is a backbone of any larger operation, not only IT, and we can't properly succeed without it.
  - Although DoIT does have IT policies of their own, it is imperative that the agencies also have their own policies. DoIT's policies do not automatically apply to the agencies.

- Objective B:
  - Second objective emphasizes protection of information through proper backup process and encryption. As a state we do not want to lose data that is paramount to its operations and we want to protect that data from unauthorized use by encrypting it.
  - Security: We are only as good as our weakest link. We are the keepers of the states information, including citizen's (and our own) personal information.
  - Responsibility: While DoIT (or other hosting services) may manage backups on behalf of the agency, it is the agencies responsibility to make sure they have procedures of their own to make sure their backups are completed, working and accurate from their end. If something were to go wrong, it is still their data, and their responsibility.

- Objective D

- The emphasis is ensuring that we are developing a accountable, secure and functional system for its users. A lot goes into the development of even a simple application; these controls are best practice for simple applications but are imperative for complicated applications.
- For major new systems and major modifications to current systems, internal audit should be doing a Pre-implementation review.

- Objective E
  - This objective is looking at critical function applications or financial implication applications. Larger agencies can consider doing this review for multiple applications.
  - Rotating what is reviewed gives the agency a broader idea of what weakness may exist, especially if there are legacy systems used in the agency
    - Legacy systems were developed with older technology. They may not have many functions modern systems have for security.
      - EX) Access Databases do not have encryption options built in but SQL Databases do.
  - Hosting environments create their own set of risks.

- A-9: Senior leadership is aware/approves new systems and/or modifications
  - This approval is new to the checklist. It is not enough to be aware, approval is needed.
  - A lot of resources go into these projects before and after they have started, approval gives the okay to continue the current path.

- A-13: SOC reports are important. They give a better picture into the inner workings of the development teams processes, procedures, and policies. DoIT reviewing the SOC reports is not enough. It is up to the agency to preform their own due diligence and review all relevant SOC reports. Agencies are not all alike with their infrastructure.

- A-16: PCI compliance is required for all applications **and** for all bureaus that use credit card transactions, regardless if they use the Treasure's E-pay system.
  - EX) Bureaus' A and B uses System 1 which accepts credit card transactions.
    - Both Bureau A and B need to be PCI compliant for System 1
  - EX) Bureau A uses System 1 and System 2 which both accept credit card transactions
    - Bureau A needs to be PCI compliant for System 1 and System 2.

- B-6: Disaster Recovery Plan is the plan of how to get the agency back up and working.
  - While the agency may have to rely on DoIT or 3ed parties, they still need to know what to do on their end. Each agency is different.
    - Things like who to call, hours of operation, potential workarounds, etc.

- C-1: Vulnerability Scans should to be done before any state information is moved onto a new platform or modifications to a platform. This goes back to we are only as strong as our weakest link.

New Rules and Statues in Place

(20 ILCS 450/) Data Security on State Computers Act.
https://ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2438&ChapterID=5
Disposing of EDP equipment

(5 ILCS 175/) Electronic Commerce Security Act.
https://ilga.gov/legislation/ilcs/ilcs3.asp?ActID=89&ChapterID=2

(20 ILCS 1370/) Department of Innovation and Technology Act.
https://ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3879&ChapterID=5
Creation of DoIT

(20 ILCS 1375/) Illinois Information Security Improvement Act.
https://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=002013750HArt%2E+5&ActID=3880&ChapterID=5&SeqStart=100000&SeqEnd=800000