Cyber Security Audits Framework

Kathy Lovejoy, CPA, CISA, Principal of IS Audits

The Auditor General's Office performs several types of audits:

- Performance Audits
  - Per Resolution
- Financial Audits
  - CAFR,
  - Single Audit,
  - Universities,
  - Component Units, and
  - Department level.
- Compliance Examinations
  - Departments,
  - Universities, and
  - Component Units.
- IS Audit
  - System and Organization Control Examinations (SOC 1 & SOC 2),
  - General IT Control,
  - System Developments/Project Management,
  - Cyber Security,
  - Network/Mainframe,
  - Application Reviews, and
  - Data Analysis (Medicaid/SNAP/TANF).

The Office has two Divisions

- Performance Division (25 auditors)
- Financial/Compliance Division (44 auditors, with 6 IS auditors)
  - Approximately 80% of the audits are contracted out to CPA Firms

Illinois State Auditing Act
30 ILCS 5/3-2.4

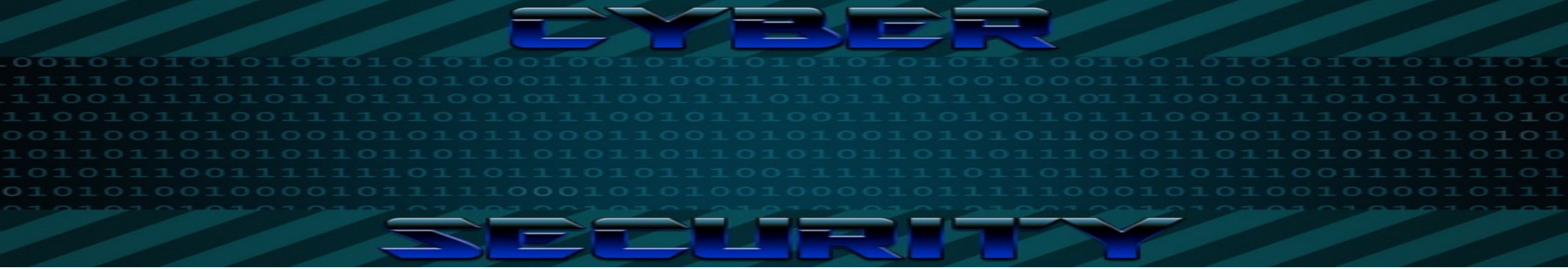
Effective January 1, 2019, the Act requires the Auditor General to review State agencies and their cybersecurity programs and practices, with a particular focus on agencies holding large volumes of personal information.

The review is to assess, at a minimum

1. the effectiveness of the State agency cybersecurity practices;
2. the risks or vulnerabilities of the cybersecurity systems used by State agencies;
3. the types of information that are most susceptible to attack
4. ways to improve cybersecurity and eliminate vulnerabilities of State cybersecurity systems; and
5. Any other information concerning the cybersecurity of State agencies that the Auditor General deems necessary and proper.

Resources Utilized to Develop Cybersecurity Program

- NIST's Framework for Improving Critical Infrastructure Cybersecurity
- NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- COBIT- Control Objectives for Information and Related Technology
- Health Insurance Portability and Accountability Act (45 CFR § 164)
- Federal laws related to the specific agency/university
- State of Illinois laws
  - Personal Information Protection Act (815 ILCS 530)
  - Data Security on State Computers Act (20 ILCS 450)
  - Identity Protection Act (5 ILCS 179)



Cybersecurity Audits Objectives

- Policies and Procedures
- Roles and Responsibilities
- Data Classification and Protection

Questionnaire

1. Have policies, procedures and processes to manage and monitor the regulatory, legal, environmental and operational requirements been established and communicated?
2. Have cybersecurity roles and responsibilities been established and documented?
3. Has a formal risk assessment been performed to identify and ensure adequate protection of information most susceptible to attack?
4. Has data been classified to establish the types of information most susceptible to attack to ensure adequate protection?
5. Have the overall risks or vulnerabilities of information systems and data been adequately assessed?

Policies and Procedures

OBJECTIVE

Determine if the Department has established security policies, processes and procedures and are utilized in the protection of assets.

TESTING

Obtain the policies to determine if they address:

- Configuration Management
- Acceptable Use
- Access Control
- Security Awareness and Training
- On-boarding policies for staff and contractors.
- System development standards.
- Change management.
- Disaster recovery and response.
- Backup verification and off-site storage.
- Data maintenance and destruction.

Policies and Procedures

OBJECTIVE

Determine if the policies and procedures are reviewed and updated on a timely basis.

TESTING

Obtain documentation to determine the Department's timeframe for reviews and when the policies were last reviewed.

Policies and Procedures

OBJECTIVE

Determine if the policies and procedures have been formally communicated to staff and contractors and they acknowledged their understanding.

TESTING

Conduct testing of staff and contractors to determine if they had been provided the policies and procedures and completed an acknowledgment indicating they understood the policies and procedures.

Policies and Procedures

OBJECTIVE

Determine if the Department has policies and procedures for reporting security violations and suspected violations.

TESTING

Obtain their policies and procedures to determine if it address reporting violations.

Policies and Procedures

OBJECTIVE

Determine if an appropriate security structure has been established and reviewed at service providers to ensure resources and data are protected.

TESTING

Obtain documentation of security structure over service providers.

Obtain documentation the internal controls of the service provider had been reviewed and assessed by the Department.

Policies and Procedures

OBJECTIVE

Determine if a project management framework has been established and implemented to ensure new applications (projects) are implemented to meet management's intentions.

TESTING

Obtain documentation of the project management framework.

Select a project to determine if the Department followed the project management framework.

OWN SECURE PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

Cybersecurity Trivia

Which of the following devices could potentially be exploited by an attacker?

- Desktop computer
- Laptop computer
- Cell phone
- Television
- Refrigerator
- Digital assistant
- Remote-controlled keys
- Tablet
- Security camera
- Pacemaker
- Baby monitor
- GPS
- Toaster
- Thermostat

Answer: All of them. Yes, even the toaster – possibly.

ATTENDANCE CODE

Roles and Responsibilities

OBJECTIVE

Determine if a security management structure has been established and if it documents responsibilities.

TESTING

Obtain and review the security management structure and determine if the associated roles and responsibilities are documented.

Roles and Responsibilities

OBJECTIVE

Determine is cybersecurity staff are aware of their roles and responsibilities.

TESTING

Obtain and review documentation of cybersecurity staff roles and responsibilities.

Interview cybersecurity staff to determine if they are aware of their roles and responsibilities.

Roles and Responsibilities

OBJECTIVE

Determine if staff and contractors have been provided cybersecurity training and understand their responsibilities.

TESTING

Obtain documentation cybersecurity training has been provided to new staff and contractors.

Obtain documentation cybersecurity training is provided at least annually to staff and contractors.

Risks and Vulnerabilities

OBJECTIVE

Determine if the Department has established a risk management methodology.

TESTING

Obtain the methodology and determine if the methodology addresses:

- Categorization of information systems
- Selection of security controls
- Implementation of security controls
- Assessment of the security controls
- Authorization of information system access
- Monitoring of security controls

Risks and Vulnerabilities

OBJECTIVES	TESTING
Determine if the Department has conducted a formal risk assessment which identified confidential, personal and information that is susceptible to attacks.	Obtain the risk assessment and determine if it identified confidential, personal, and information that is susceptible to attacks.
Determine if the Department has prioritized, evaluated and implemented appropriate risk reducing controls.	Obtain documentation of the controls and determine their prioritization, if they have been evaluated, and implemented.

Risks and Vulnerabilities

OBJECTIVES

Determine if security solutions are managed to provide security and resilience of assets.

Determine if assets are monitored to identify events.

Determine if events are detected in a timely manner and the impact is determined.

TESTING

Obtain documentation of the security solutions and if it provides security and resilience of assets.

Obtain documentation as to the events monitored for, the impact, the frequency of the review, and follow up actions.

Risks and Vulnerabilities

OBJECTIVE

Determine if response procedures have been established, documented, and are executed in response to an event.

TESTING

Obtain procedures and review to determine if they address the required actions to respond to event.

Test a sample of events to determine if the procedures were complied with.

Risks and Vulnerabilities

OBJECTIVE

Determine is user access rights are aligned with job duties.

TESTING

Obtain documentation and interview users to determine their job duties to ensure access is appropriate.

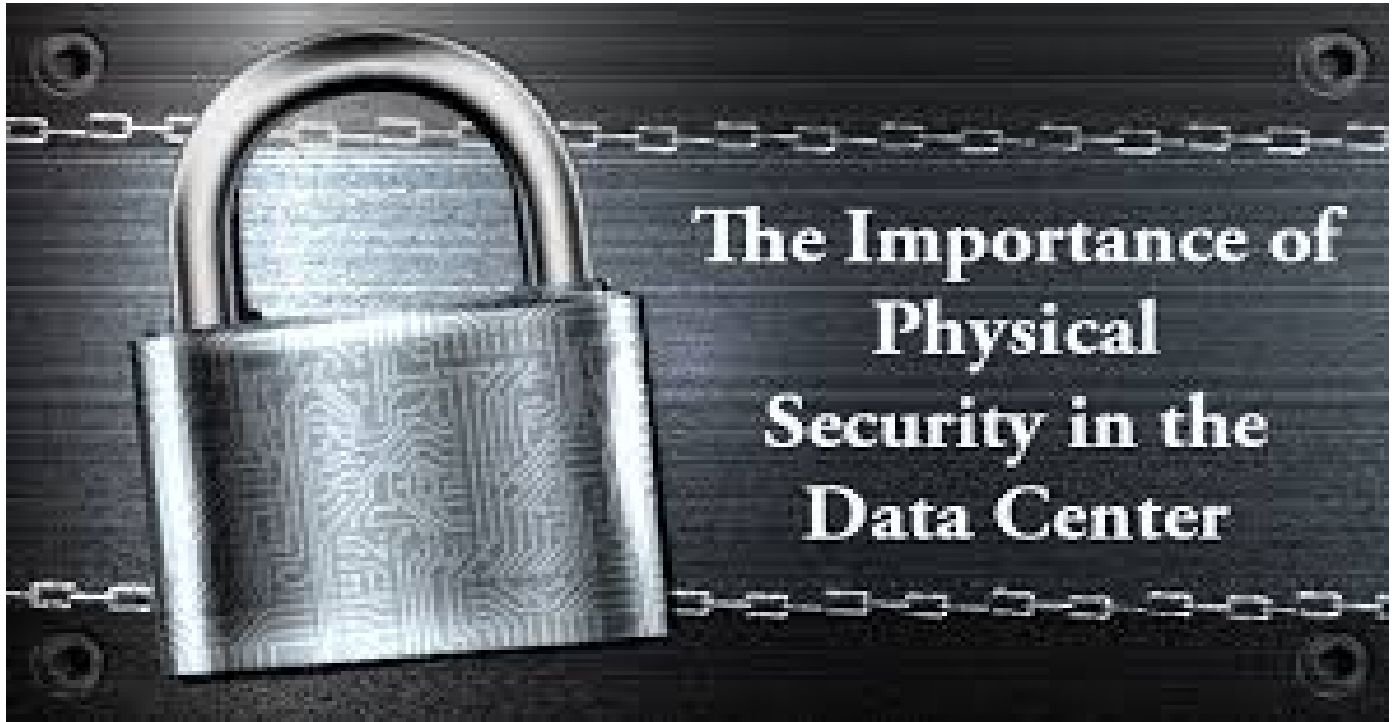
Risks and Vulnerabilities

OBJECTIVES

Determine if adequate physical security controls are in place to protect assets.

TESTING

Document the physical security controls in place over the Department's critical assets.



Data Classification and Protection

OBJECTIVE

Determine if the Department has established a data classification methodology.

TESTING

Does the methodology address:

- Classification based on risk?
- Associated protection based on classification?
  - Categories (.i.e. public, sensitive, confidential, personal)
  - Storage Media
  - Access Permissions
  - Data Retention
  - Data Destruction

Data Classification and Protection

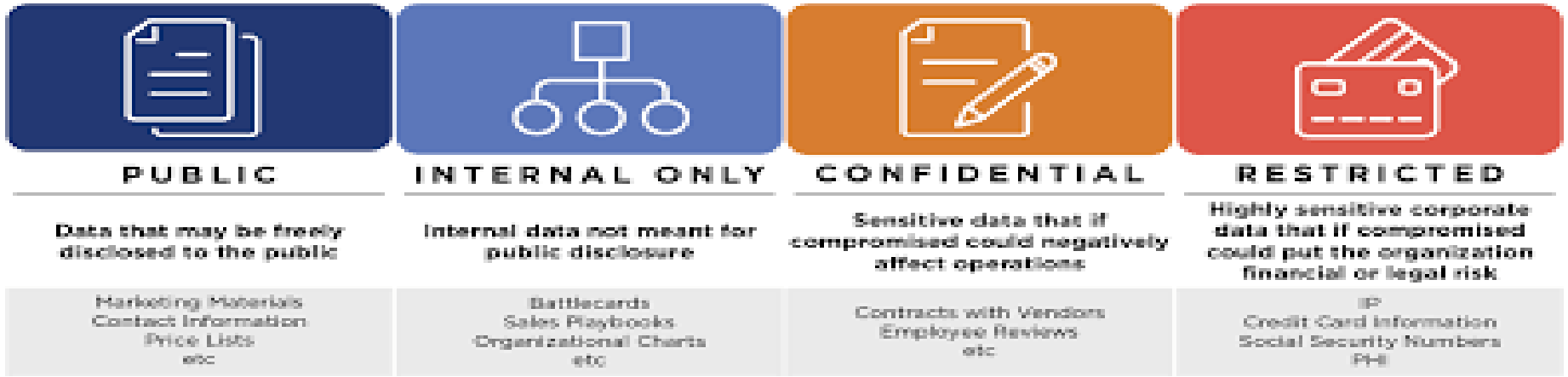
OBJECTIVE

Determine if data is managed and classified in accordance with the risk strategy.

Determine if all types of data have been identified and classified to ensure proper safeguards.

TESTING

Obtain documentation that data has been classified and determine if it is in accordance with the risk strategy.



Results and Findings

- For Fiscal Year 2019, ten agencies which hold large volumes of data had significant weaknesses which resulted in findings.
  - Had not established a formal framework including assigned responsibilities over cybersecurity.
  - Had not developed policies regarding the reporting of security violations or suspected violations.
  - Had not classified their data to identify and ensure adequate protection of information most susceptible to attack.
  - Had not evaluated and implemented appropriate controls to reduce risk.
  - Had not ensured all staff completed cybersecurity training upon employment and annually thereafter.
  - Had not developed a formal, comprehensive, adequate, and communicated security program to manage and monitor the regulatory, legal environment, and operating requirements.

OWN SECURE PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

Approximately how many attempted cyber attacks are reported by the Pentagon every day?

Answer: Over 10 million.

OWN SECURE PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

How many unfilled cybersecurity jobs are there in the United States alone?

Answer: 310,000.

CONTACT INFORMATION

Kathy Lovejoy: Klovejoy@auditor.Illinois.gov or (217) 782-6046