MaherDuessel

Pursuing the profession while promoting the public good©

www.md-cpas.com

Information Technology Risks

Agenda

1. Understanding IT Audit Risks
2. Access Controls
3. Disaster Recovery
4. Third Party/Vendor Controls
5. Final Thoughts

Why the BIG deal?

- Digital world
  - Cashless, email, logging in to client portals
- Accuracy of records
  - Eliminate human errors
- Audit Requirement
  - Understanding of the informational technology controls of an Auditee

Context

Data
The management relies on an application system or data warehouse to process or maintain data (e.g. transactions or other relevant data) related to significant accounts or disclosures or reports used in the operation of relevant control.

Automated Controls
The management relies upon the application system to perform certain automated functions that are relevant to the audit.

System-Generated Reports
The management relies on an application, data warehouse query, or report writer to generate a report that is used in the operation of relevant controls.

Our Guidance

- Annual IT checklist
  - Additional follow-up and testing performed over the IT checklist
  - User Access Controls
  - Overall technology environment at the Organization we are auditing
- Additional risks over remote environment which is now a normal aspect of business

IT Service Provider

- Does your Organization contract out IT or does your Organization have in-house IT?

- In-house: Is there sufficient knowledge on the IT team, Is the workload manageable?

- Contracted: Is there an official agreement with the third party?

Specific Risks

- PCI DSS- Credit Card information
  - Stored/processed onsite vs. third party
- HIPPA/Hi-Tech
  - Protected information normally related to Healthcare type data, far reaching
- Gramm-Leach-Bliley Act
  - Educational and financial institutions additional qualifications necessary

Accounting Software

- Type and functionality
  - Automatic vs manual operations
  - Access to the accounting software
  - Documentation of those rights
  - Review of those rights
- Overall network security and individual application security

Access Controls

Access Controls

- A component of data security that dictates who is allowed to utilize company information and resources
- “Front-door” access: legitimate access to data from applications and their functionality
- “Back-door” access: accessing raw data directly through tools other than the application
  - This can be staff members or positions in IT

Access Controls

- **Authorization access controls** have the goal of ensuring that the person seeking access is authorized, most often done with login credentials
- **Authentication access controls** attempt to ensure that persons logging in to the system are who they say they are, such as with biometrics
- Insiders in the company are responsible for just as many security incidents as outsiders
- Employees should only have need-to-know access to be able to do their jobs and nothing more

Audit Scope

Includes those systems impacting financial statements. Typically accounting software, billing, membership database, donor database, portals for payroll and pension plan information

Access Control Audit Impact

- Access control deficiency:
  - Material weakness
  - Inappropriate persons have access to electronically approve invoices (role-based access)
    - Tested all material invoices for non-routine vendors instead of a sample of 25 invoices
  - Payroll clerk inappropriately has access to payroll portal (segregation of duties)
    - Add detail testing of the payroll clerk's pay to audit program

Poll

- What is the recommended password/ passphrase character length?
  - 8
  - 10
  - 12
  - 15

Poll

Which Password is the best choice:

. aPpI3P!367*

- Ilovetoswim123!
- D&fkl68$)
- snowswimmingbluechair

Poll

- What is the best measure to protect your password:
  - Change your password frequently
  - Utilize special characters
  - Enable Multi-Factor Authentication
  - Use a long and complex passphrase

Passwords

- NIST Guidance on passwords
  - No longer recommends requiring regular password resets
  - Use multi-factor authentication
  - Screen passwords
  - Limit failed password attempts
  - Use salt and hash to protect passwords

Passwords

- To be reliable, passwords should:
  - be a minimum of eight characters
  - Be a mix of lowercase letters, uppercase letters, numbers and special characters to increase the strength of the password
  - automatically logoff or timeout due to inactivity
  - lock out of the account after three failed attempts (the duration of the lock out should be around 60-90 minutes to frustrate hacker attempts, it could be indefinite for more sensitive accounts requiring reestablishment of credentials)
  - be removed or disabled for terminated employees’ credentials in a timely manner
- There should also be a segregation of duties (SoD) so that the person responsible for password policies, settings, and configurations should not be entering data or having access to applications

Access Determination

- Who determines access
  - Data Owner vs IT
- Level of Access
  - Is it role-based or ad hoc, structured access is best practice, exceptions should be minimal
- Review of those who have access
  - Should be performed on a yearly basis at a minimal

Server and NOS

- “shares” should be examined and used sparingly/judiciously
- Rights to the server should be restricted for each group and user
- The vendor should have read only and temporary access to maintain/debug the server. Sanitize default account credentials.

OS, DBA, and Network Admin.

- They have back door access based on the nature of their function
- There should be a limit on the number of people with such rights
- A small Organization should have roughly 2-3
- DBA pose more of a risk factor as they know more about the data

Third-Party Applications

- Vendor Access:
  - Vendors generally focus on ease of use rather than internal control
  - It is important to understand the vendor's access prior to the use/implementation of the software, such as its ability to create, change, or delete user IDs/data
  - All activity performed by the vendor should be logged and reviewed by the Organization

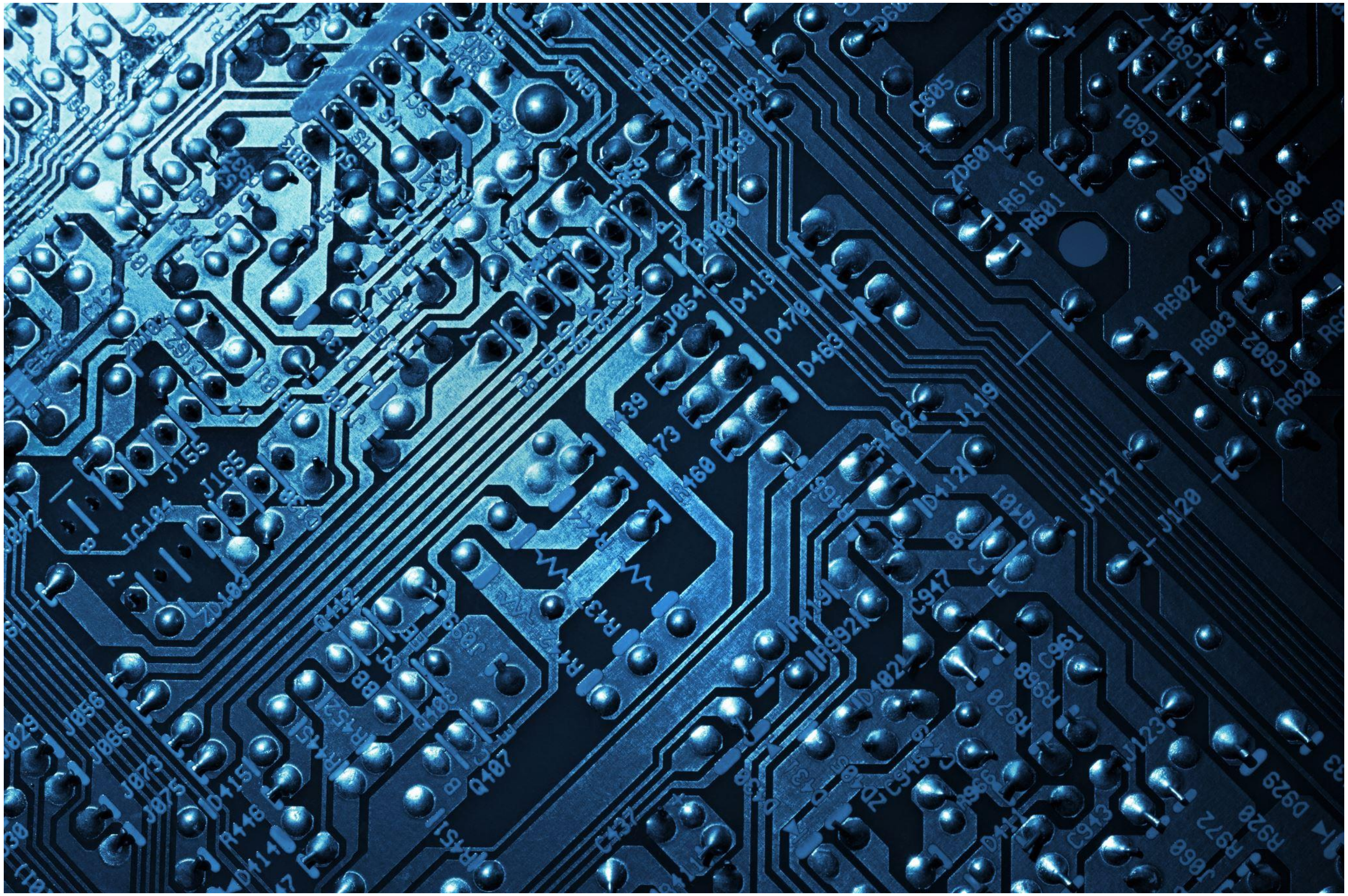
Third-Party Applications

- Vendor Procedures:
  - When a vendor performs work for the organization, a user audit trail is necessary to monitor the vendor’s actions
  - The audit trail can not have the ability to be altered by the vendor or the Organization’s system administrator

Retention

- Does the Organization maintain passwords or other identifiable information
- Retaining Access Audits
- Access for groups, if role based
- How is user access terminated and/or changed from original set up

Disaster Recovery



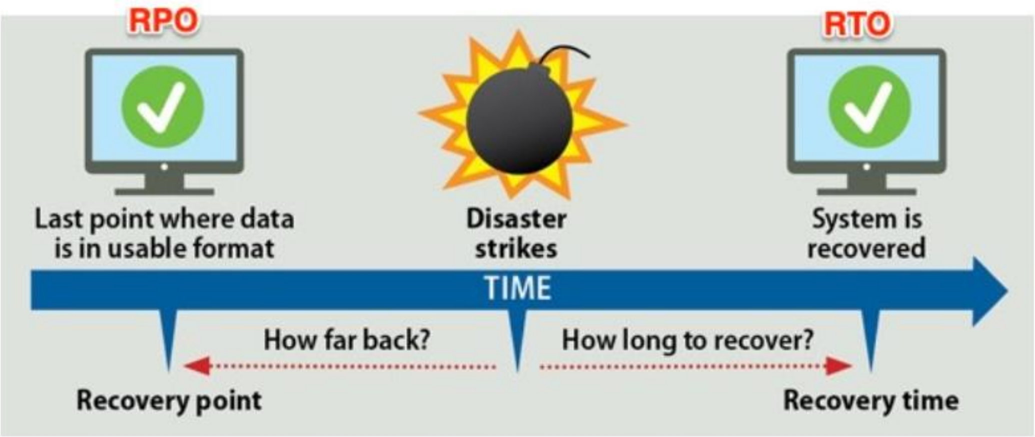
Disaster Recovery

- The ability to recover from an adverse event over the Organization’s IT infrastructure
  - Environmental
  - Physical
  - Internal
  - Malicious
- Object is to have the appropriate RPO and RTO for Organization based on value

RTO and RPO

- RTO Recovery Time Objective
  - Maximum acceptable delay between interruption of service and restoration of service
    - How long can you be down

- RPO Recovery Point Objective
  - Maximum acceptable amount of time since the last data recovery point
    - How much are you willing to lose



Other Disaster Mitigators

- Cyber Security Insurance- covers losses in the event of an adverse event
  - Cost prohibitive
  - Not all events are covered and/or offered
- Testing of any plan that is determined to be necessary and retention of that test

Performing Arts Organization

- Asset: 3rd party web-based ticketing system
- What could go wrong? Ticketing system not available
  - Ensure download of daily sales including seat
  - Ensure copy of current seating chart
  - Follow previously developed procedures to utilize secondary vendor or in –house box office

How to Lower Insurance

- Implement a strong password control policy and make certain you follow it. Include dual authentication.
- Encrypt sensitive data and personally identifiable info
- Control the number of records you access, store and transfer - don’t store PII, Credit Card info – use a 3rd party?

Back Ups

- Full back ups
- Incremental back ups
- Who performs them, where are these back ups stored (Cloud is physical location)
- Are these tested, if hosted what happens if you change provider
- This is critical to the disaster recovery process

Security

- Physical security of information technology
- Software security - are patches and updates automatically applied
- Network security - firewalls, routers, intrusion detection, data encryption, etc.
- Cyber Security training provided
  - Phishing, best practices, etc.

IT Governance

- Is there an IT committee on the board of directors, or other governance committee
- Vendor maintenance - ensure your vendors are reliable, has there been any security issues at these vendors?
- Has the Organization been made aware of any actual incidences of cyber incidents

Outside Vendors

Reliance on Outside Vendors

- Does your Organization rely on outside vendors for internal controls or processing?
- Payroll outsourced for processing, investments, health insurance, etc.
  - How do you know that their controls are working appropriately ?
  - Do you have the controls you need at your Organization to ensure that the third party is working correctly (complimentary)?

Vendor Control

- Must obtain, review, and understand the third-party Organization's controls and controls that should be in place at your Organization
- SOC reports (Service Organization Controls) - this is performed by an independent agency, think audit for controls
- Any issues should be reviewed by management and should ensure complimentary controls are in place

Service Organization Control Reports

- SOC 1 Report: provides information about the controls at a Service Organization that may directly impact its financial statements
  - Examples: Maintenance accounting software, custodian for investment companies, mortgage services or depository institutions that service loans for others

Service Organization Control Reports

- SOC 2 Report: provides information about the suitability of the design and controls at the Service Organization relevant to security, availability, processing integrity, confidentiality, or privacy
  - Examples (for SOC 3 as well): Hosting and support services (cloud computing, IT infrastructure, data center management), sales force automation, health-care claims management and processing

Service Organization Control Reports

- SOC 3 Report:
  - covers the same principals as SOC 2
  - without the detailed understanding of the design of controls and tests performed by the service auditor
  - This report provides the auditor’s opinion on whether the Service Organization maintains effective controls over its systems and is typically intended for users who do not require a more thorough report

Service Organizations

- Factors important for Service Organizations:
  - Nature and authority of external information
  - Ability of management to influence information obtained
  - The competence and reputation of the external information source
  - Past experience of the auditor with the reliability of the information
  - Evidence of general market acceptance by users of the relevant information
  - Whether the entity has in place controls to address the relevance and reliability of information

What To Look For?

- Opinion
- Subservice Organizations
  - Vendor used by your Service Organization to perform services that are likely to be relevant to those user entities' internal control
- Breaches/incidents
- Complementary user entity controls (CUEC's) – controls that you have in place in order to properly use the service contracted
  - Access
  - Providing accurate info
  - Reviewing reports

Final Thoughts!

Common Audit Issues Encountered

- Terminated and/or transferred employees continue to have access
- Appropriate role-based access
- Poor password management - easy to guess passwords, written passwords, sharing of passwords
- Poor general user education

Issues (continued)

- Direct change access
- Third-party IT service provider
  - Needs to lay out what the IT service provider is responsible for
- Password/authentication management

What Should I Be Asking About?

Harvard Bus review March 4, 2020 by Dr. Keri Pearlson and Nelson Novaes Neto:

- What are the Organization’s most important assets and how are we protecting them? (personal data of students, credit cards, healthcare records)
- What are the layers of protection we have put in place? (perimeter security, encryption)
  - Was a risk assessment performed? What were the results?
- How do we know if we’ve been breached? How do we detect a breach?
- What are the response plans in the event of an incident?
  - Will you pay ransom?

What Should I Be Asking About?

- How is it communicated?   Which authorities get notified (HIPPA- are there contracts or other agreements in place? If your vendor notifies you that your info is breached?)
- What is the board's role in an incident? Support a public announcement? Decide on paying ransom?
- What are our business recovery plans in the event of a cybersecurity incident?

What Should I Be Asking About?

- Is our cybersecurity investment enough?
  - Simulations of cyber-attacks and penetration/ vulnerability tests

More Information

NIST : WWW.NIST.GOV

- National Institute of Standards and Technology
- Non-regulatory agency of the Department of commerce
- Offers guidelines on technology-related matters

NIST

- NIST Special Publication 800-63B: Digital Identity Guidelines (Updated 2020)
- NIST Special Publication 800-184: Guide For Cybersecurity Event Recovery

Questions

Shawn Strauss CPA, CISA, CITP

sstrauss@md-cpas.com