



A Practical Approach to Cybersecurity Risk Mitigation

Javier Young, CISSP
Principal, Cybersecurity Services Group
CLA (*CliftonLarsonAllen LLP*)
November 16, 2022

Disclaimer

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Learning Objectives

Develop	Develop a framework of knowledge to plan for future security efforts
Learn	Learn where organizations can focus valuable risk mitigation resources
Understand	Understand the importance of business continuity planning
Recognize	Recognize the components of the incident response process
Understand	Understand risks associated with commercial off-the-shelf (COTS) products

About CLA

CLA exists to create opportunities for our clients, our people, and our communities through industry-focused wealth advisory, digital, audit, tax, consulting, and outsourcing services.

With more than 7,500 people, 121 U.S. locations, and a global vision, we promise to know you and help you. For more information visit CLAconnect.com. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.





The Framework

www.cisecurity.org/controls

Policies and Standards

People, Rules and Tools

- What do we expect to occur?
- How do we conduct business?

Standards based operations from a governance or compliance framework:

- CIS Critical Controls, NIST, ISO

CIS Controls - V8

CONTROL 01 Inventory and Control of Enterprise Assets

5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5

CONTROL 02 Inventory and Control of Software Assets

7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7

CONTROL 03 Data Protection

14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software

12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12

CONTROL 05 Account Management

6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6

CONTROL 06 Access Control Management

8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8

CONTROL 07 Continuous Vulnerability Management

7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7

CONTROL 08 Audit Log Management

12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12

CONTROL 09 Email and Web Browser Protections

7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7

CONTROL 10 Malware Defenses

7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7

CONTROL 11 Data Recovery

5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5

CONTROL 12 Network Infrastructure Management

8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8

CONTROL 13 Network Monitoring and Defense

11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11

CONTROL 14 Security Awareness and Skills Training

9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9

CONTROL 15 Service Provider Management

7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7

CONTROL 16 Applications Software Security

14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14

CONTROL 17 Incident Response Management

9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9

CONTROL 18 Penetration Testing

5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5



Inventory and Control of Enterprise Assets

- Understand what hardware you have/own
 - Workstations
 - Servers
 - Mobile devices
 - Internet of Things (IoT) devices

Inventory and Control of Software Assets



Understand what software you have/own



Develop an approved products list

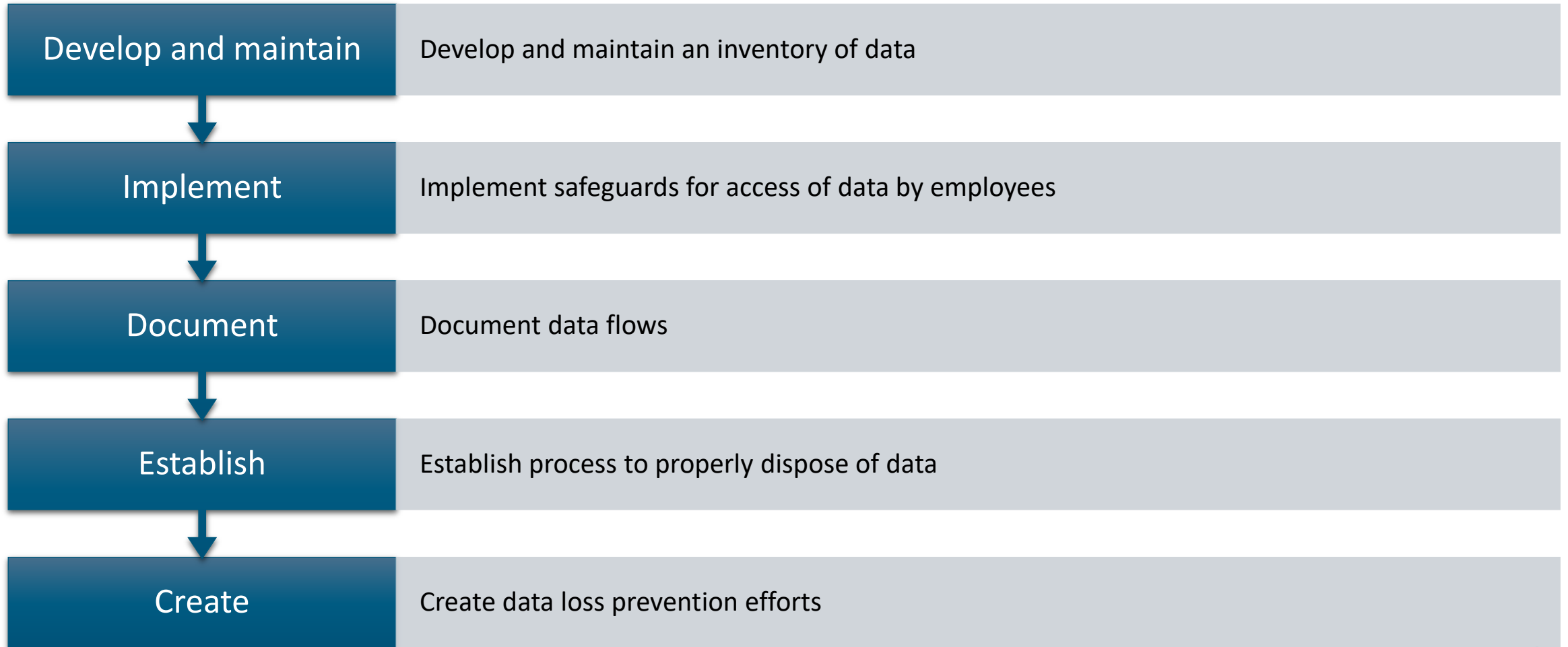


Ensure software is supported by vendor and apply latest patches



Address unauthorized software

Data Protection



Secure Configuration of Enterprise Assets and Software

- *“Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).”*

Account Management

01

Identify and inventory all accounts in the organization

02

Establish policies for use of strong and unique passwords

03

Review users to ensure they are authorized and have the correct access rights

04

Disable/delete dormant accounts

Access Control Management

01

Establish proper user access granting process

02

Develop proper user access revocation process

03

Practice least privilege with user accounts

04

Utilize role-based access methods

05

Require multi-factor authentication, especially for external services

CIS Benchmarks



With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

[Join a Community](#)

[Overview of CIS Benchmarks and CIS-CAT Demo](#)

[Register for the Webinar](#)
Tue, Oct 25, at 1:30pm EDT
Tue, Nov 15, at 10:30am EDT

[CIS Benchmarks FAQ](#)

- Operating Systems
- Server Software
- Cloud Providers
- Mobile Devices
- Network Devices
- Desktop Software
- Linux
- Microsoft Windows
- UNIX
- IBM

Currently showing Microsoft Windows benchmarks [Go back to showing ALL](#)

[Operating Systems](#) **Microsoft Intune For Windows 10** [Download CIS Benchmark](#) →

[Microsoft Windows](#) [Expand to see related content](#) ↓





Business Continuity

Business Continuity Planning

Continuity event planning and preparedness

Responsibilities and communication plans

Alternate procedures for critical business processes while systems/applications and facilities are unavailable

Alternate locations/facilities where work can commence during disaster situation

Recovery strategies and procedures for critical systems/applications.


Continuity planning for key technology service providers and vendor-hosted systems/applications

Planning for a Pandemic



Plan the Test and Test the Plan!

The BCP should be tested such that every critical component is tested at least once every three years (systems, processes)



A test plan should show scheduled testing for the current year



BCP testing should include networking, hosts, personnel, and procedures.



Incident Response Planning

The Incident Response Lifecycle

Preparation

Identification

Containment

Eradication

Recovery

Lessons
Learned

Preparation

Can we properly respond to comprehensive security incidents?

Create incident response policies

Develop roles and responsibilities

Establish communication procedures

Ensure we have the correct people, process, and tools/technologies in place

Identification

Detection and Analysis

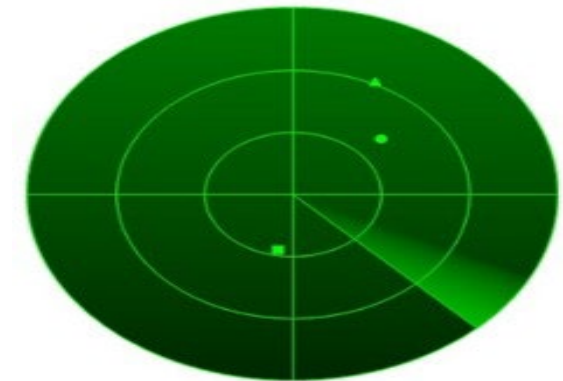
- Analyzing of logs
- Proper alerting based on abnormal activity
 - Unusual files
 - Unusual process
- New accounts created

Triage and Escalation

- Is this truly an incident that we need to respond to?
- Escalate to proper personnel
- Follow chain of custody

System and Vulnerability Management and Monitoring

- Monitoring (built in)
 - Key system configurations
 - System and application logs
 - Accounts
 - Critical data systems/files
 - Data activity and flow
- Scanning (independent)
 - Patch Tuesday and vulnerability scanning
 - Rogue devices



Containment



Eradication

Confirm root cause



Remove malware



Wipe/Format/Rebuild



Apply necessary patches



Ensure no other footholds exist



Implement proper firewall/IDS/IPS rules

Recovery

01

Continue to monitor
for indicators of
compromise

02

Search for and
ensure attacker
artifacts are gone

03

Return to normal
state of operations

Lessons Learned



Document incident



Report to necessary stakeholders



Ensure protections are in place to mitigate same type of incident occurs



Modify process(es), if needed

Incident Response Preparedness



Unfortunately, data breach can still occur despite implementing all the best security precautions



When that occurs, organizations need to ensure they are ready to respond to a data breach.



Have a plan, practice the plan, prove the plan

Have a Plan

Develop an incident response plan

- Include the appropriate procedures
- Ensure points of contact are included
- Keep the plan update to date

Establish relationships with key incident responders

- Breach Counsel
- Forensic provider
- Public relations

Practice the Plan

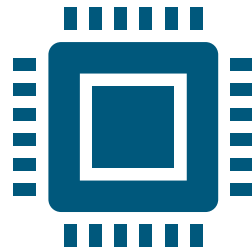
- Like all emergency procedures, they need to be practiced
- Table-top exercises- simulations where participants walk through the incident and response procedures
- Two types of table-top exercises
 - Technical
 - Management
- Both types should be conducted annually



Prove the plan



Many businesses end up over-notifying customers about data breaches, significantly increasing costs and risk of litigation



Low visibility into IT infrastructure means lack of forensic evidence to determine which system or data hackers accessed



Conduct trial forensic exercises to ensure you have the proper data and visibility

Incident Response Preparedness- Cost Savings



Impact of 25 key factors on the average total cost of a data breach
Change in US\$ from average total cost of \$3.86 million

By the numbers:

- \$8.64m – Average cost of a data breach in the United States



Source: IBM Security Cost of a Data Breach Report 2020



Commercial Off-The-Shelf (COTS) Software

COTS – Strengths and Gotchas

Strengths

Normally takes care of a need without a heavy lift internally

- Buy vs build

Many vendors will install the product and provide training to staff

Gotchas

- Not one size fits all
- Must educate staff to manage product or outsource administration
- Must be consistently tuned for effectiveness



Questions?

Contact Javier Young
javier.young@CLAconnect.com