Welcome to

Systems Security - 3

Intro to IT-security 2024

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

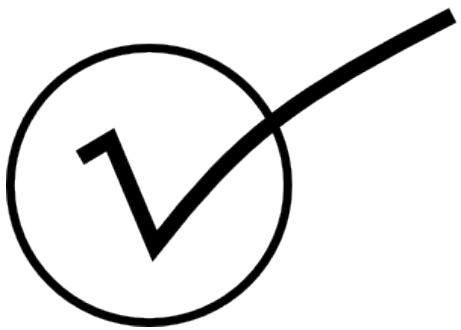
Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/
intro-to-it-security-system-security-3.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: xhek@kea.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Goals for part I



- Benchmarking and Auditing
- See some example standards – helpful for generic security planning
- Talk about auditing infrastructure security as a whole – a holistic view
- Try using our knowledge from an auditing viewpoint

Exercises

- Debian Linux exercises

Photo by Thomas Galler on Unsplash

Building Secure Infrastructures

kea

A real-life setup of an infrastructure from scratch can be daunting!

You need:

- Policies
- Procedures
- Incident Response

Running systems which require

- Configurations
- Settings
- Supporting infrastructure – networks
- Supporting infrastructure – logging, dashboarding, monitoring

Building something *secure* is **hard work!**

Existing infrastructures

or even worse you inherited an infrastructure

Multiple networks, with different vendors, rules

Multiple generations of services, applications, technologies

Built over decades

Varying to no documentation

Organizational challenges

Ingrained culture – frozen in time

How do you get started improving security?

Security Controls and Frameworks

Multiple exist

- CIS controls Center for Internet Security (CIS) https://www.cisecurity.org
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
- NIST Cybersecurity Framework (CSF)
  Framework for Improving Critical Infrastructure Cybersecurity
  https://www.nist.gov/cyberframework
  http://csrc.nist.gov/publications/PubsSPs.html
- National Security Agency (NSA)
  http://www.nsa.gov/research/publications/index.shtml
- NSA security configuration guides
  http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
- Information Systems Audit and Control Association (ISACA)
  http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx

Risk management defined

Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. ***Information risk management (IRM)*** is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

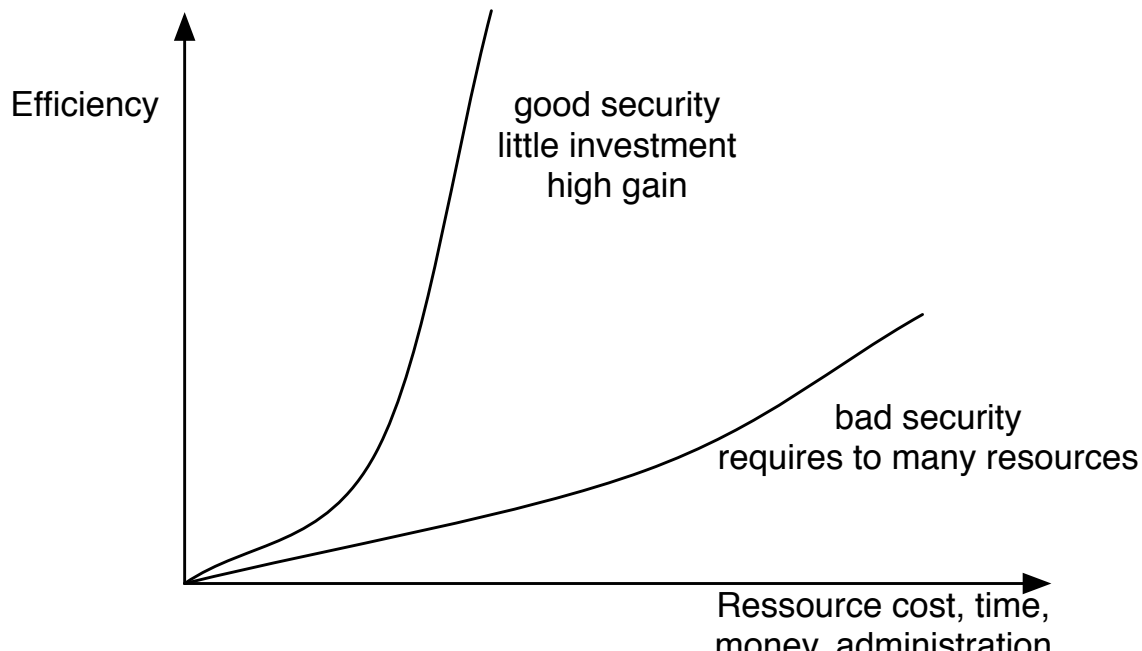
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Note: these still have errors and bugs, but are better than older versions

OpenBSD has shown the way in many cases
http://www.openbsd.org/papers/

Always try to make life worse and more costly for attackers

Good security



You always have limited resources for protection - use them as best as possible

First advice

Use technology

Learn the technology - read the freaking manual

Think about the data you have, upload, facebook license?! WTF!

Think about the data you create - nude pictures taken, where will they show up?

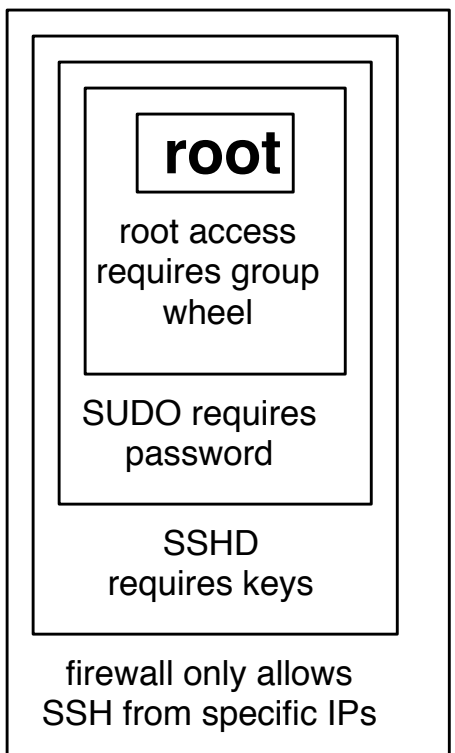
- Turn off features you don't use
- Turn off network connections when not in use
- Update software and applications
- Turn on encryption: IMAP**S**, POP3**S**, HTTP**S** also for data at rest, full disk encryption, tablet encryption
- Lock devices automatically when not used for 10 minutes
- Dont trust fancy logins like fingerprint scanner or face recognition on cheap devices

Spearphishing - targetted attacks

Spearphishing - targetted attacks directed at specific individuals or companies

- Use 0-day vulnerabilities only in a few places
- Create backdoors and mangle them until not recognized by Anti-virus software
- Research and send to those most likely to activate program, open file, visit page
- Stuxnet is an example of a targeted attack using multiple 0-day vulns

Defense in depth - flere lag af sikkerhed



Defense using multiple layers is stronger!

Integrate or develop?

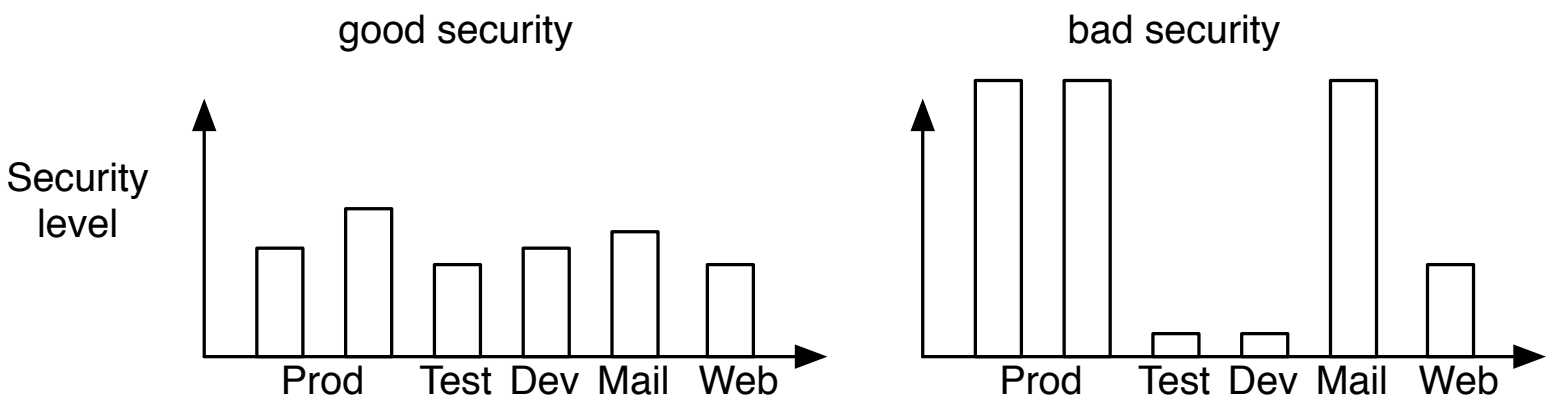
Dont:

- Reinvent the wheel - too many times, unless you can maintain it afterwards
- Never invent cryptography yourself
- No copy paste of functionality, harder to maintain in the future

Do:

- Integrate with existing solutions
- Use existing well-tested code: cryptography, authentication, hashing
- Centralize security in your code and organization

Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

How to become secure

Dont use computers at all, data about you is still processed by computers :-(

Dont use a single device for all types of data

Dont use a single server for all types of data, mail server != web server

Configure systems to be secure by default, or change defaults

Use secure protocols and VPN solutions

As said by Bruce Schneier *Security is a process, not a product.*

https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Center for Internet Security CIS Controls

> The CIS ControlsTM are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

Source: https://www.cisecurity.org/ CIS-Controls-Version-7-1.pdf

Center for Internet Security CIS Controls 7.1

- The five critical tenets of an effective cyber defense system as reflected in the CIS Controls are:
- **Offense informs defense:** Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
- **Prioritization:** Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups discussed below are a great place for organizations to start identifying relevant Sub-Controls.
- **Measurements and Metrics:** Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- **Continuous diagnostics and mitigation:** Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.
- **Automation:** Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics. Source: CIS-Controls-Version-7-1.pdf

Inventory and Control of Hardware Assets

CIS controls 1-6 are Basic, everyone must do them.

> CIS Control 1:
> Inventory and Control of Hardware Assets
> Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

What is connected to our networks?

What firmware do we need to install on hardware?

Where IS the hardware we own?

What hardware is still supported by vendor?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Inventory and Control of Software Assets

CIS Control 2:
Inventory and Control of Software Assets
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

What licenses do we have? Paying too much?

What versions of software do we depend on?

What software needs to be phased out, upgraded?

What software do our employees need to support?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Continuous Vulnerability Management

CIS Control 3:
Continuous Vulnerability Management
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Controlled Use of Administrative Privileges

CIS Control 4:
Controlled Use of Administrative Privileges
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Secure Configuration for Hardware and Software

CIS Control 5:
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

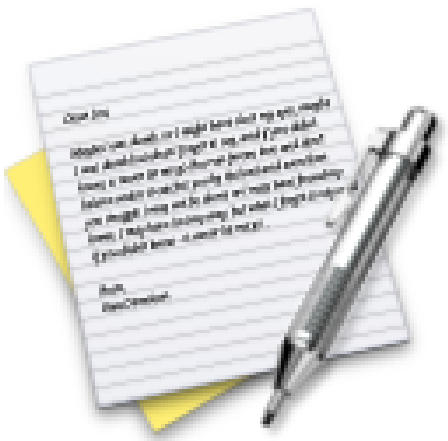
Maintenance, Monitoring and Analysis of Audit Logs

CIS Control 6:
Maintenance, Monitoring and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

... and present it, use it daily, report it to management!

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Exercise

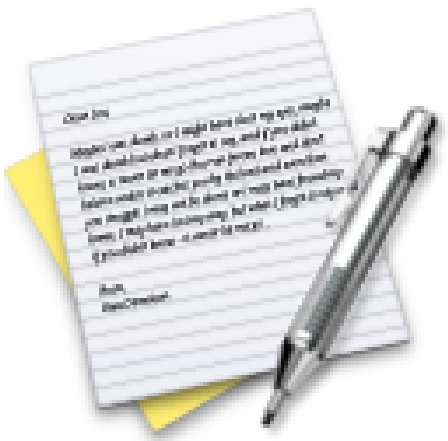


Now lets do the exercise

⚠ CIS Benchmarks 30min

which is number **19** in the exercise PDF.

Exercise

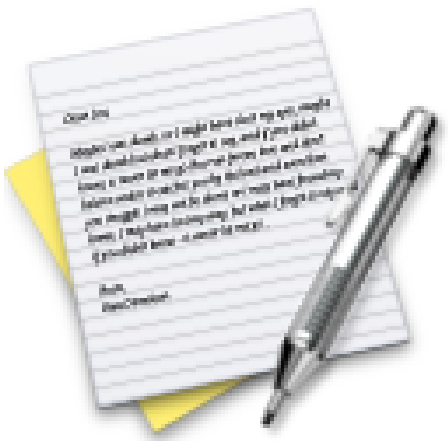


Now lets do the exercise

⚠ Lynis Auditing, System hardening, and Compliance testing 30min

which is number **20** in the exercise PDF.

Exercise



Now lets do the exercise

ℹ SSH scanners 15min

which is number 21 in the exercise PDF.

End of part I

Take a break!

Goals part II: Increase Security Awareness

Continue with Auditing and Benchmarking

We will skip most of the remaining CIS slides, you can use them later

Email and Web Browser Protections

CIS controls 7-16 are Foundational

> CIS Control 7:
> Email and Web Browser Protections
> Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Use centralized proxies, with filtering settings?

Automated browser updates

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Malware Defenses

CIS Control 8:
Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Also included network segmentation in my book

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Limitation and Control of Network Ports, Protocols, and Services

kea

CIS Control 9:
Limitation and Control of Network Ports, Protocols, and Services
Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers

Monitor the network using netflow, internally too!

Why does some server on the inside connect to Internet Relay Chat (IRC)

Do we still run older versions of Server Message Block (SMB) services

Why haven't we turned off Telnet on the network devices?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Data Recovery Capabilities

CIS Control 10:
Data Recovery Capabilities
The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Secure Configuration for Network Devices

CIS Control 11:
Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Boundary Defense

CIS Control 12:
Boundary Defense
Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Data Protection

CIS Control 13:
Data Protection
The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Yes, EU General Data Protection Regulation (GDPR)

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Controlled Access Based on the Need to Know

CIS Control 14:
Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Wireless Access Control

CIS Control 15:
Wireless Access Control The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Account Monitoring and Control

CIS Control 16:
Account Monitoring and Control
Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Implement a Security Awareness and Training Program

CIS controls 17-20 er Organizational

> CIS Control 17:
> Implement a Security Awareness and Training Program
> For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Application Software Security

CIS Control 18:
Application Software Security
Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Incident Response and Management

CIS Control 19:
Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Penetration Tests and Red Team Exercises

CIS Control 20:
Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

CIS RAM

CIS Risk Assessment Method is a free information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls™ cybersecurity best practices. CIS RAM provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

Tools are available, sometimes tool is just a spreadsheet for recording data

Payment Card Industry Data Security Standard

PCI Best Practices grew out of credit card leaks becoming a huge problem

Partnership between Master Card, VISA and others

Version 1.0 release in December, 2004

Version 3.2.1 was released in May 2018
https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

PCI DSS Control Objectives

High level objectives:

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS Resources

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources to assist organizations with their PCI DSS assessments and validations, including:

Document Library, including:

- PCI DSS – Summary of Changes from PCI DSS version 2.0 to 3.0
- PCI DSS Quick Reference Guide
- PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms
- Information Supplements and Guidelines
- Prioritized Approach for PCI DSS
- Report on Compliance (ROC) Reporting Template and Reporting Instructions
- Self-assessment Questionnaires (SAQs) and SAQ Instructions and Guidelines
- Attestations of Compliance (AOCs)

Frequently Asked Questions (FAQs)

PCI for Small Merchants website

PCI training courses and informational webinars

List of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)

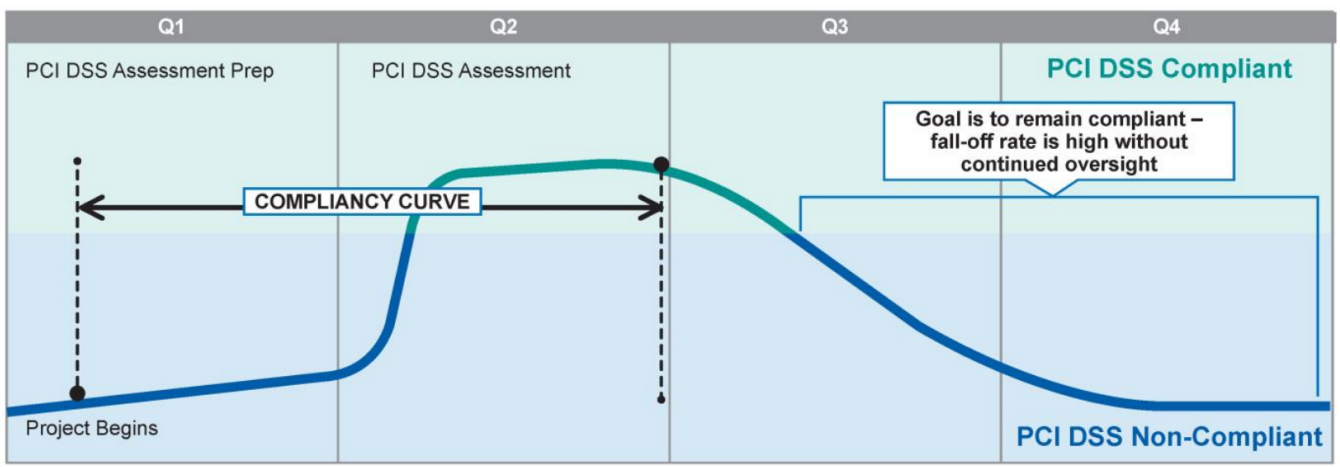
List of PTS approved devices and PA-DSS validated payment applications

Note: Information Supplements complement the PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements — they do not supersede, replace or extend the PCI DSS or any of its requirements. Please refer to www.pcisecuritystandards.org for information about these and other resources.

Source: Payment Card Industry (PCI) Data Security Standard version 3.2.1 May 2018

Challenges to Maintaining Compliance

Figure 1: Compliancy Curve



Source: *Information Supplement: Best Practices for Maintaining PCI DSS Compliance*, 2.0 Date: January 2019, Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council

Requirements for Building and Maintaining Security

Installing and maintaining a firewall configuration to protect cardholder data. The purpose of a firewall is to scan all network traffic, block untrusted networks from accessing the system.

Changing vendor-supplied defaults for system passwords and other security parameters. These passwords are easily discovered through public information and can be used by malicious individuals to gain unauthorized access to systems.

Protecting stored cardholder data. Encryption, hashing, masking and truncation are methods used to protect card holder data.

Encrypting transmission of cardholder data over open, public networks. Strong encryption, including using only trusted keys and certifications reduces risk of being targeted by malicious individuals through hacking.

Source: *Information Supplement: Best Practices for Maintaining PCI DSS Compliance*, 2.0 Date: January 2019, Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council

Requirements for Building and Maintaining Security, cont

Protecting all systems against malware and performing regular updates of anti-virus software. Malware can enter a network through numerous ways, including Internet use, employee email, mobile devices or storage devices. Up-to-date anti-virus software or supplemental anti-malware software will reduce the risk of exploitation via malware.

Developing and maintaining secure systems and applications. Vulnerabilities in systems and applications allow unscrupulous individuals to gain privileged access. Security patches should be immediately installed to fix vulnerability and prevent exploitation and compromise of cardholder data.

Source: *Information Supplement: Best Practices for Maintaining PCI DSS Compliance*, 2.0 Date: January 2019, Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council

Requirements for Building and Maintaining Security, cont

Restricting access to cardholder data to only authorized personnel. Systems and processes must be used to restrict access to cardholder data on a "need to know" basis.

Identifying and authenticating access to system components. Each person with access to system components should be assigned a unique identification (ID) that allows accountability of access to critical data systems.

Restricting physical access to cardholder data. Physical access to cardholder data or systems that hold this data must be secure to prevent the unauthorized access or removal of data.

Tracking and monitoring all access to cardholder data and network resources. Logging mechanisms should be in place to track user activities that are critical to prevent, detect or minimize impact of data compromises.

Source: *Information Supplement: Best Practices for Maintaining PCI DSS Compliance*, 2.0 Date: January 2019, Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council

Requirements for Building and Maintaining Security, cont

Testing security systems and processes regularly. New vulnerabilities are continuously discovered. Systems, processes and software need to be tested frequently to uncover vulnerabilities that could be used by malicious individuals.

Maintaining an information security policy for all personnel. A strong security policy includes making personnel understand the sensitivity of data and their responsibility to protect it.

Source: *Information Supplement: Best Practices for Maintaining PCI DSS Compliance*, 2.0 Date: January 2019, Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council

Benefits of PCI DSS

My opinion:

Before PCI theres was a LOT of breaches

Minimum requirements for credit card companies, should be minimum requirements for personal data

Good requirements, a library of tested requirements

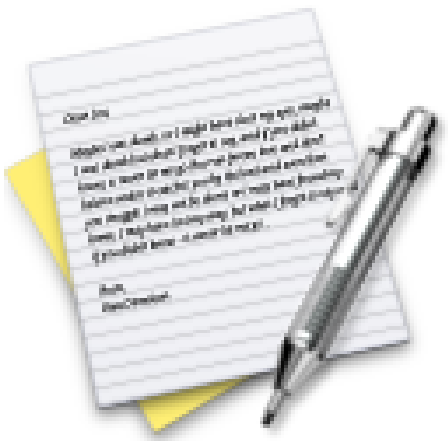
Exercise

Now lets do the exercise

Example Policies up to 25min

which is number 22 in the exercise PDF.

Exercise



Now lets do the exercise

⚠ Centralized syslog 30min

which is number 23 in the exercise PDF.