Governance and Compliance

Cybersecurity

GRC Unit, Day 3

Class Objectives

By the end of today’s class, you will be able to:

- Explain how organizations use policy and procedure to formalize standards of “right” and “wrong”.
- Use governance frameworks to determine which policies an organization must develop.
- Explain how audits are used to ensure compliance.
- Develop business continuity and disaster recovery plans.

DAY 1

Structure of the security and the importance of a strong security culture

DAY 2

Threat Modeling and Risk Analysis

Governance and Compliance

Today we will cover governance, compliance, and business continuity planning and disaster recovery.

Governance

Codifying and enforcing proper behavior and operations, i.e. establishing standards of “right” and “wrong”, and enforcing those standards.

Compliance

Enforcing the policies in order to meet those standards.

Knowledge of governance, compliance, and BCP/DR is crucial context for all security professionals because **most of security professionals work is mandated by governance policies and subject to compliance audits**.

Class Breakdown

Today’s class will proceed as follows:

01 Codifying Rules with Policy and Procedures

02 Using Governance Frameworks to Guide Policy Decisions

03 Understanding Audit and Compliance

04 Business Continuity Planning and Disaster Recovery

05 Developing BCP/DR Recommendations for an Organization

Codifying and Enforcing Behavior with Policies and Procedures

Review:

This week we developed a training plan to improve *GeldCorp's* security culture.

This training plan was meant to protect the organization by changing employee *behavior*.

It defined the **policy** or“right behavior”; i.e. what employees *should* do when faced with suspicious links

Policy <> Frameworks <> Compliance <> Audits

How are they connected?

Organizations use **policies** to define standards for behavior and operations.

Each individual policy is just one rule amongst many. In practice, organizations will have many policies to support a given goal. For example, a company must have many security policies in place to protect its data.

Guidelines for which kinds of policies an organization should have in place are called governance frameworks.

Governance frameworks describe which guarantees a company must provide to remain compliant with federal regulations and industry standards.

Audit is the process of checking whether an organization is compliant with a given framework or guideline

Today’s Scenario

In today’s activities, we will:

- Define formal policies for *GeldCorp*
- Assess what user data collected by *GeldCorp* is subject to GDPR and PCI
- Determine whether *GeldCorp's* data collection practices are GDPR and PCI compliant

Refresher on our GeldCorp Training Plan

We developed our training plan by setting a **goal**, and determining the necessary steps to achieve it.

The training plan prescribed a specific rule employees should follow: Do not click on links to domains outside of the corporate intranet.

This rule is an example of a ***policy***, which is a course or principle of action proposed by a business. In this case, the rule specifies a download policy.

The goal of defining and implementing a new download policy was to reduce employee click-through rate to less than 5%. **In other words, the business implemented policy as a means of achieving this goal.**

Business Goals Often Drive Policy Implementation

Two Categories of Business Goals

01 Internal Defined

Targets that the business sets in its own interest.

For example, an organization might aim to reduce long-term security expenses to less than $400,000.

02 External Defined / Imposed

These are targets that the business must hit because they will suffer consequences if they do not.

Examples include the requirement that emerchants handle all credit card transactions securely, under penalty of law in the event of a breach of customer PII.

Internal Objectives and Policy

Example: Reduce unauthorized root-level login incidents on Domain Controllers to 0.

Goals which are not required by any external organization or actors

An organization would hand this off the IT team, who would be responsible for determining how best to implement it.

One possible implementation is to require all Domain Administrators to use strong passwords, and force them to create a new password every month.

Password Policy

A *password policy* might require that Administrators create passwords with:

□ At least 16 Characters

□ At least 1 Letter and 1 Number

□ At least 1 Special Character (', (,], etc.)

□ No portion of the administrator's username

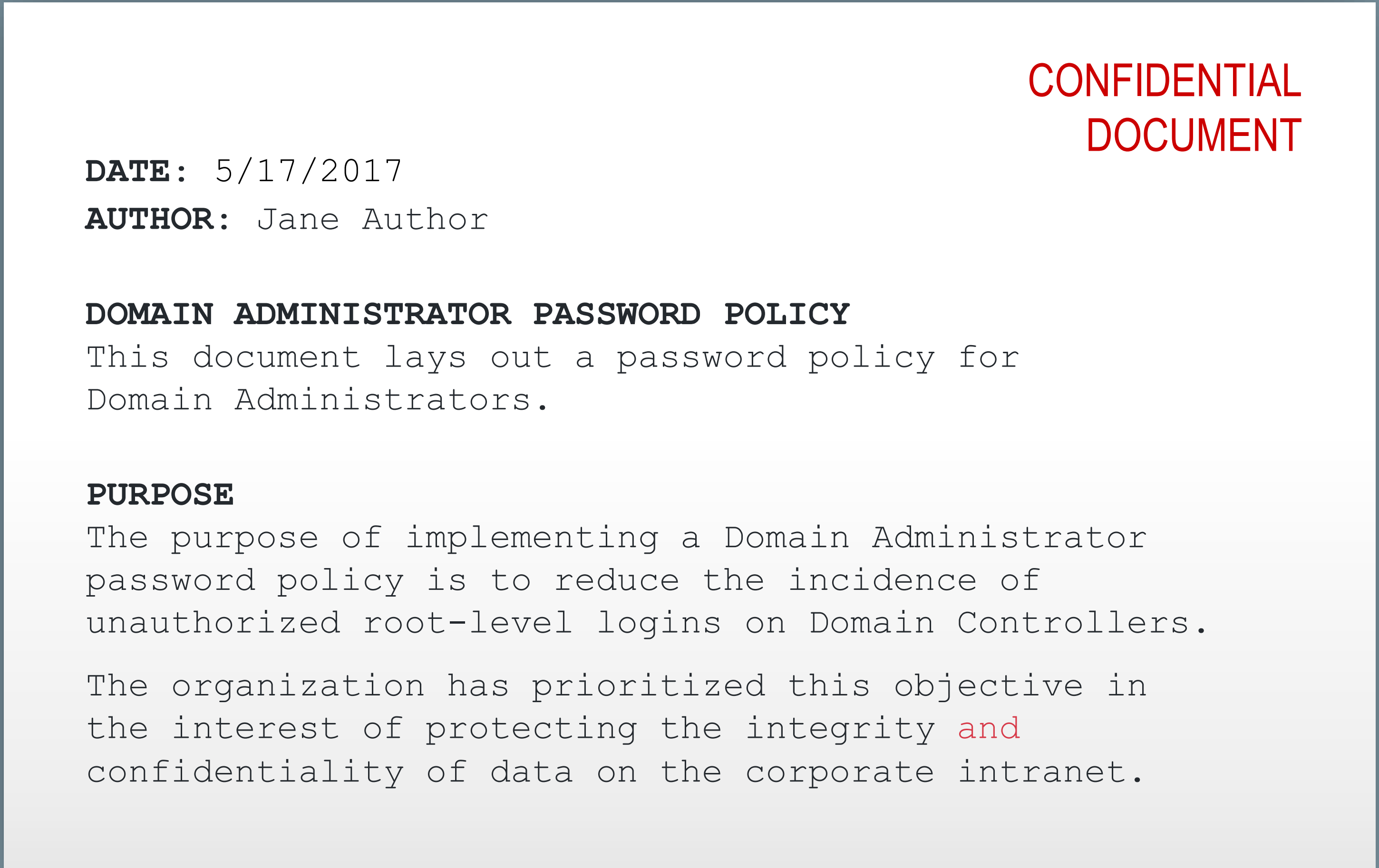
□ Passwords are also updated every month

This policy defines clear standards of behavior:

Administrators are expected to follow very specific rules with regard to their passwords, which their computers will enforce.

These rules are also specifically designed to achieve the goal of reducing the incidence of unauthorized root-level logins on Domain Controllers to 0.

Password Policy Example
(Part 1)



CONFIDENTIAL
DOCUMENT

DATE: 5/17/2017

AUTHOR: Jane Author

DOMAIN ADMINISTRATOR PASSWORD POLICY

This document lays out a password policy for Domain Administrators.

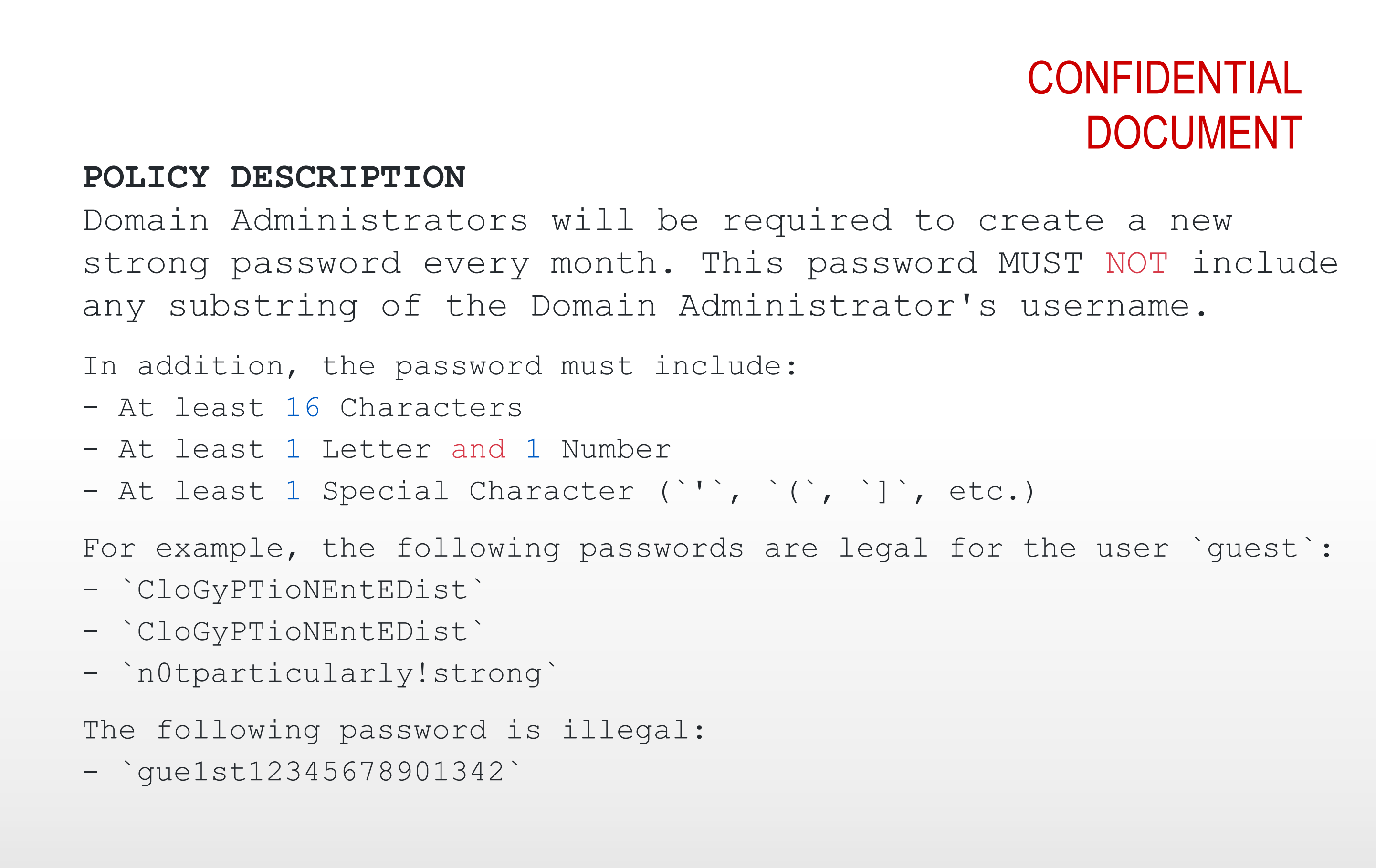
PURPOSE

The purpose of implementing a Domain Administrator password policy is to reduce the incidence of unauthorized root-level logins on Domain Controllers.

The organization has prioritized this objective in the interest of protecting the integrity and confidentiality of data on the corporate intranet.

Password Policy Example

(Part 2)



CONFIDENTIAL
DOCUMENT

POLICY DESCRIPTION

Domain Administrators will be required to create a new strong password every month. This password MUST NOT include any substring of the Domain Administrator's username.

In addition, the password must include:

- At least 16 Characters
- At least 1 Letter and 1 Number
- At least 1 Special Character (`'`, `(`, `]`, etc.)

For example, the following passwords are legal for the user `guest`:

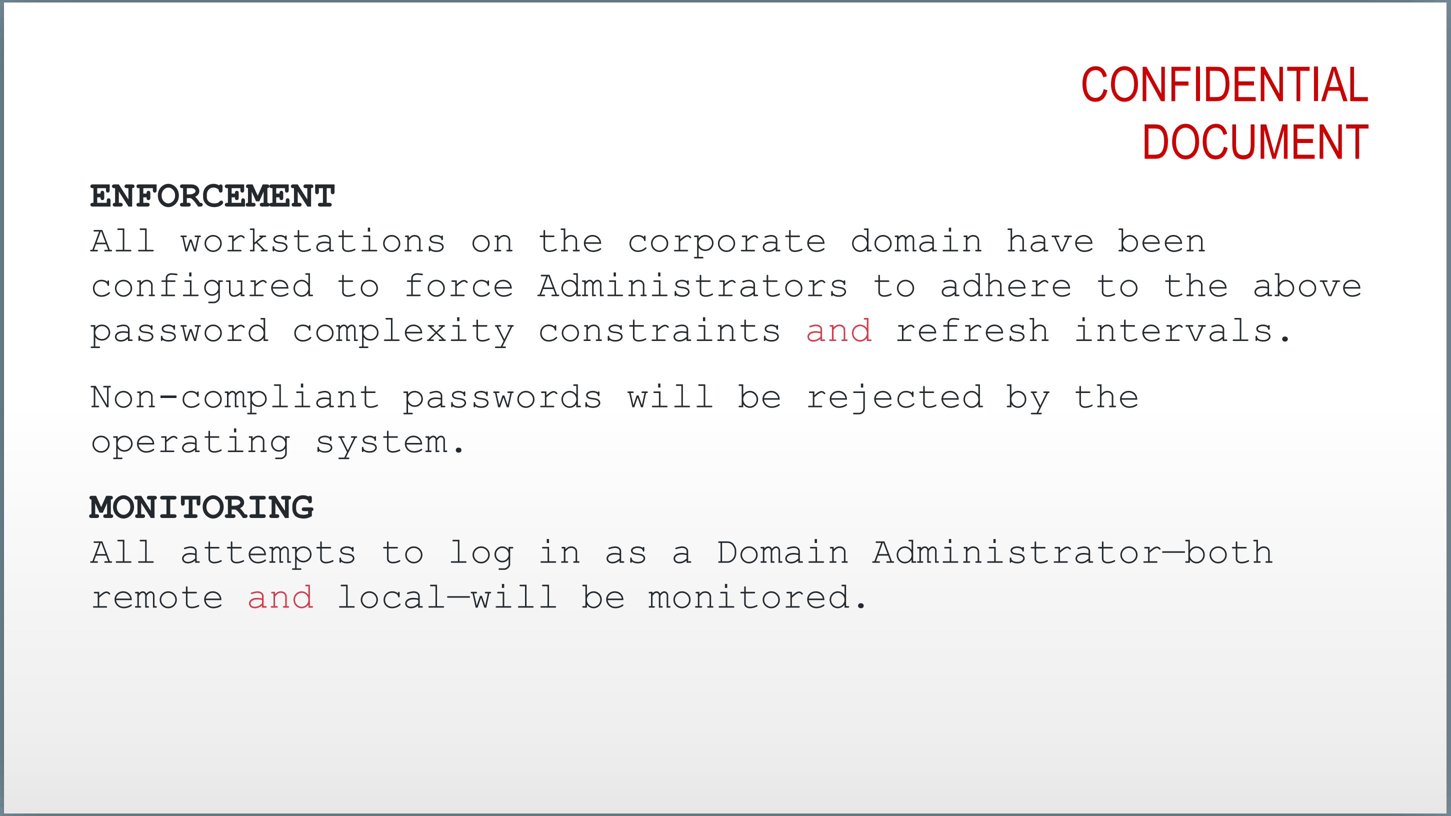
- `CloGyPTioNEntEDist`
- `CloGyPTioNEntEDist`
- `n0tparticularly!strong`

The following password is illegal:

- `gue1st12345678901342`

Password Policy Example

(Part 3)



CONFIDENTIAL
DOCUMENT

ENFORCEMENT

All workstations on the corporate domain have been configured to force Administrators to adhere to the above password complexity constraints and refresh intervals.

Non-compliant passwords will be rejected by the operating system.

MONITORING

All attempts to log in as a Domain Administrator—both remote and local—will be monitored.

Documenting Company Policies

In the previous lesson, you performed a risk analysis to help GeldCorp gain visibility into its most prominent threats. Since then, they've used your results to set numerous internal security goals.

In this exercise, you will help them realize these goals by developing and documenting policies to support them.

Suggested Time:
15 minutes

Your Turn: Password Policy

Assignment:

Work in pairs on creating a policy for the below internal goal and don't hesitate to ask your instructional staff and/or classmates for help if you get stuck.

Internal Goals

- Eliminate tailgating at all main offices.
    - Note: *Tailgating* is when an employee holds the door open for others, thus allowing them to enter the building without scanning their ID.
- Guarantee 99% uptime for all trading applications.
- Reduce incidence of developers accessing customer PII that they don't need for their projects.

Your Turn: Password Policy

Password Policy Template:

DATE:

AUTHOR:

<Policy Name>

PURPOSE

What security benefit does this policy bring?

DESCRIPTION OF <Policy Name>

What are the terms of the policy?

ENFORCEMENT

How will this policy be enforced?

MONITORING

How will the effectiveness of this policy be measured?

Times Up! Let’s Review.

Using Framework
to Guide Policy Development

Internal Objectives and Policy

Businesses often have to follow rules in addition to those they set for themselves. These rules don’t directly benefit the business, but might be mandated by the law or industry standards.

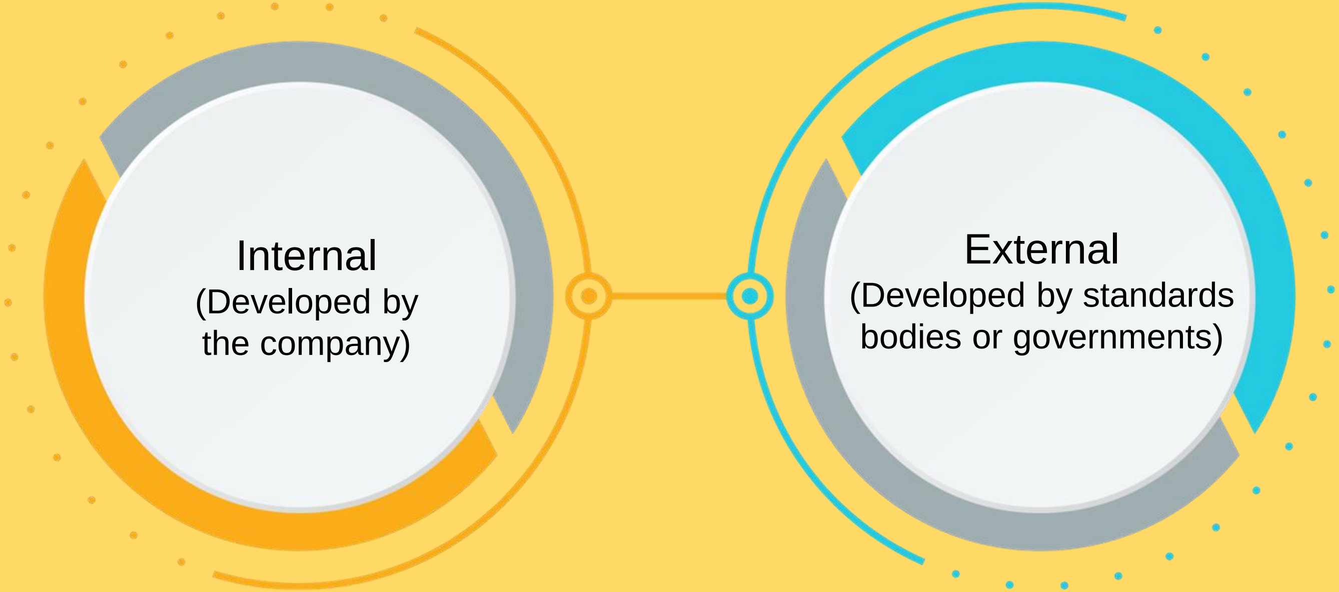
Example: Merchants that process financial transactions are legally required to guarantee that their customers’ data remains confidential. If a company suffers a breach that results in the disclosure of customer PII, they may be subject to fines and other legal penalties.

Governance Frameworks

These rules that everyone should follow are often described as policies that everyone should have in place.

Such prescriptions of which rules an organization should follow are often called **governance frameworks.**

Frameworks can be:



Internal
(Developed by the company)

External
(Developed by standards bodies or governments)

SEC

These frameworks have their origins in statutes adopted by the **Securities and Exchange Commission (SEC)**, the regulatory body in charge of enforcing and proposing laws regarding financial instruments (stocks, bonds, options, etc.), and protecting consumers from fraud.

During the 90s, the SEC worked with Congress to pass anti-fraud statutes to discourage many incidents of cybercrime.

In 2000, the SEC moved past simple anti-fraud laws by adopting a regulatory statute called Regulation S-P.

Rule 30 of Regulation S-P (Safeguard Rule)

In 2000, the SEC moved past simple anti-fraud laws by adopting a regulatory statute called Regulation S-P. This regulation did not focus entirely on security, but Rule 30 of Regulation S-P mandated that organizations establish written policies and procedures that are designed to:

Insure the security and confidentiality of customer records and information.

Protect against any anticipated threats or hazards to the security or integrity of customer records and information.

Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Regulation S-AM (August 2009)

Regulation S-AM placed limits on when corporations could share consumers' private information for advertising and marketing purposes.

Disclosure Guidance (October 2011)

On October 13 2011, the SEC issued guidelines for when and how organizations should disclose breaches of cybersecurity. While not formal regulatory statutes with the force of law, these guidelines mark an important step towards cyber regulation.

When the guidelines were released, the federal government still had no formal regulations around cybersecurity or cyber incidents, but the disclosure guidance specified that businesses were still obligated to disclose cybersecurity breaches under then-current SEC rules, if the breach resulted in the disclosure of information that a ""reasonable investor would consider important to an investment decision".

Regulation S-ID (April 2013)

Also known as ***Identity Theft Red Flags Rule***

Regulation S-ID laid forth "final rules and guidelines to require certain regulated entities to establish programs to address risks of identity theft."

- First regulation to formally require corporations to protect consumers' Non-Public Information (NPI).

Regulation S-ID obligates firms to do two things:

1. Protect against identity theft
2. Verify that requests to change an account holder's registered address indeed come from the account holder themselves.

Cybersecurity Regulation Blueprint (April 15 2014)

The SEC officially recognized cybersecurity as an exam priority, meaning that they would consider a firm's security posture as a routine part of their evaluations and audit standards.

The blueprint provides examples of the kinds of questions the SEC would ask brokerages and asset managers during audits.

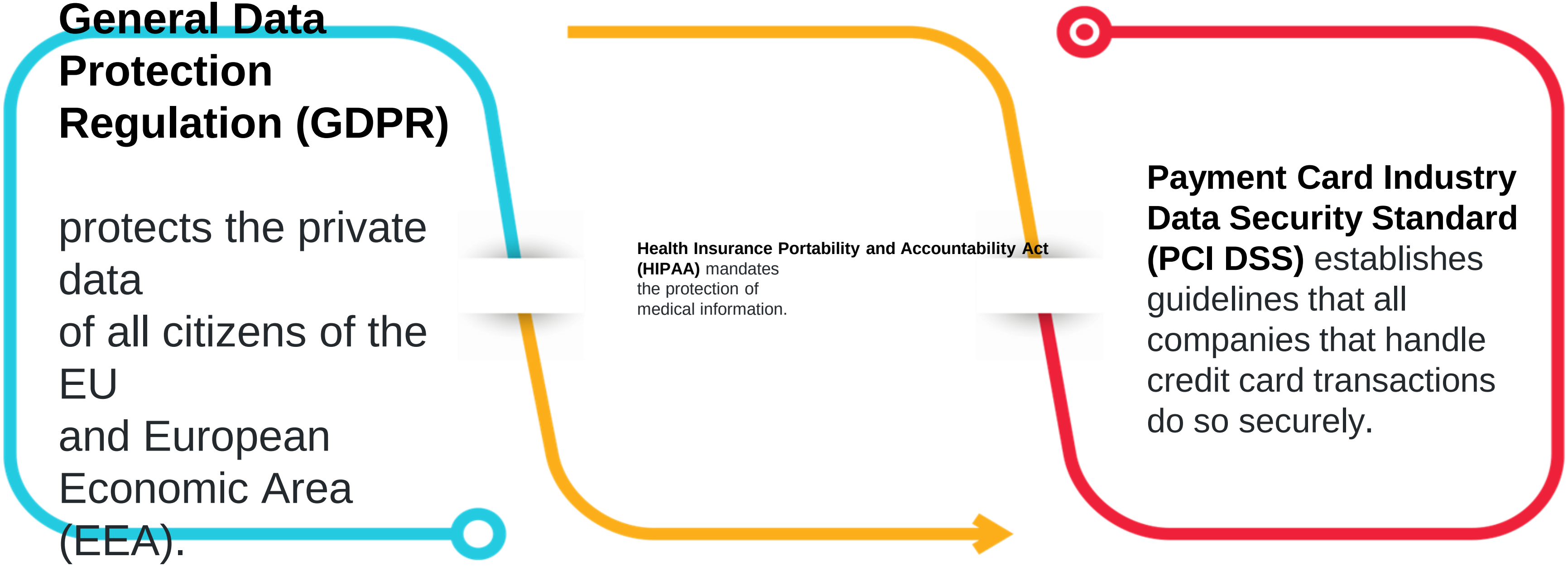
Though these statues, regulations, and guidelines were developed for financial institutions, they apply to all publicly traded organizations, regardless of industry.

While they explain what kinds of protections companies are obligated to provide their customers, they do not specify how they should meet those obligations

Governance frameworks codify standards that all businesses should follow. Since businesses in different industries manage different kinds of data, there are different frameworks for different industries.

Common Governance Frameworks

All security professionals must be familiar with the following, at minimum:



General Data Protection Regulation (GDPR)

protects the private data of all citizens of the EU and European Economic Area (EEA).

Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of medical information.

Payment Card Industry Data Security Standard (PCI DSS) establishes guidelines that all companies that handle credit card transactions do so securely.

GDPR

It requires that organizations that process data belonging to EU citizens protect the data sufficiently.

GDPR regulations apply to organizations based in the EU, as well as those based elsewhere that process data belonging to EU citizens.

HIPAA

Title II: HIPAA Administrative Specification.

Establishes privacy standards around electronic access to healthcare data. Organizations must uphold the following standards to remain HIPAA compliant:

- National Provider Identifier Standard: All healthcare entities (people, healthcare providers, health plans, and employers) must have an ID, called the National Provider Identifier (NID).
- Transactions and Code Set Standard: This standardizes health insurance claims.
- HIPAA Privacy Rule: Establishes standards protecting individually identifiable health information, such as prescription information and lab results. This defines what data to protect.
- HIPAA Security Rule: Sets standards for patient data security. This defines how well data should be protected.
- HIPAA Enforcement Rule: Establishes guidelines for investigations of non-compliant providers.

PCI

It is an organizational standard, and applies to both public and private organizations that accept, transmit, or store credit card data.

PCI defines different compliance "levels".

Companies that handle many transactions must have a stricter level of compliance than smaller ones.

The most important data protected by PCI includes:

- Cardholder Name, Expiry Date, and 3-Digit Service (CVV) Code
- Magnetic Strip Data
- PIN Numbers

Frameworks mostly describe which policies organizations should have in place, but do not specify how they should implement them.

A business's *internal policies* document *how* they choose to implement these mandates

GDPR Compliance

In this exercise, you'll explore the GDPR framework, and determine which data managed by *GeldCorp* is subject to its regulations.

Suggested Time:
15 minutes

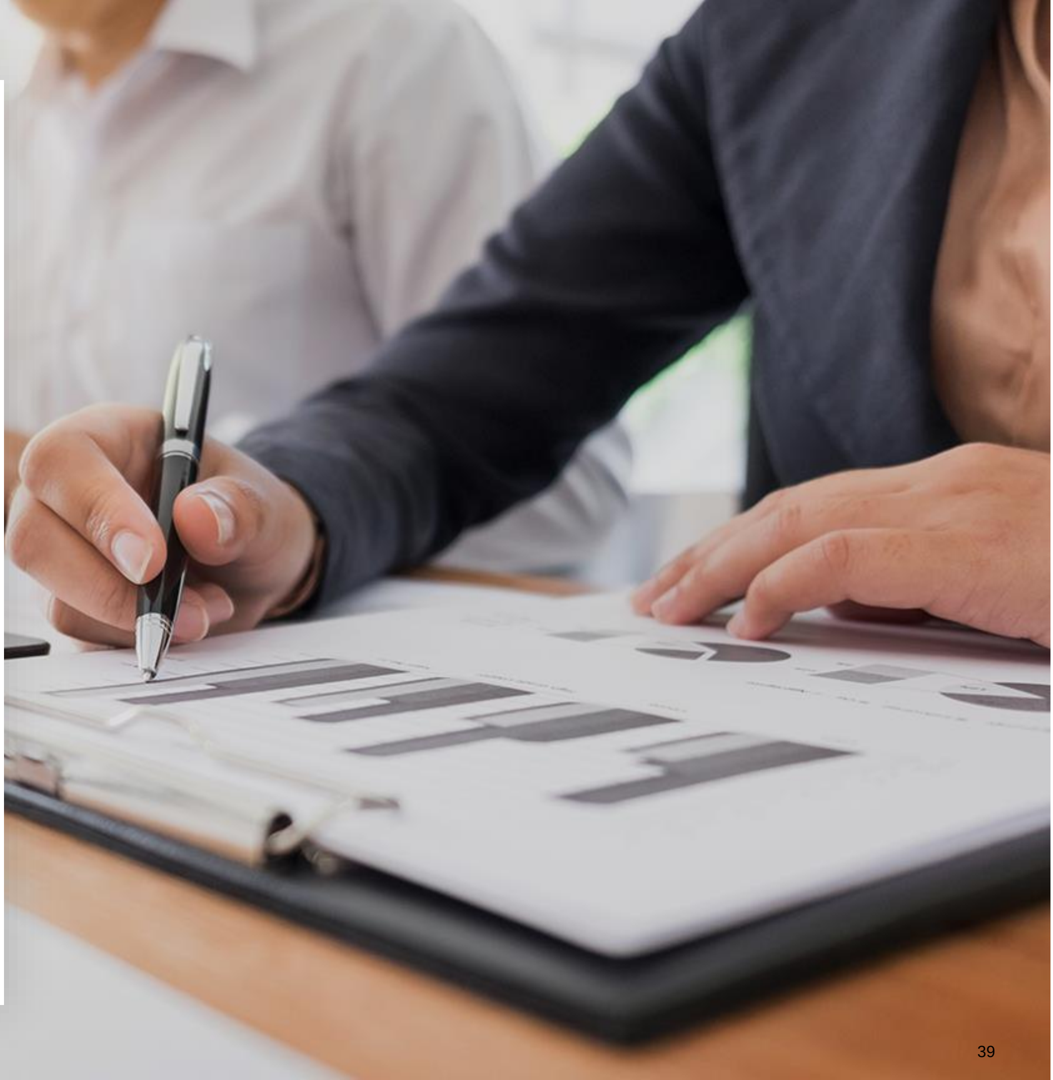
Compliance and Audit

Compliance and Audit

Business must enforce policies in order to guarantee **compliance** with legal matters.

An **audit** is the process of checking how well an organization is adhering to its policies.

- Audits are typically conducted to ensure that an organization does indeed uphold the statutes required of it by government frameworks.



Performing an Audit

Auditors refer to each rule in the framework, and check that the business is following it.

If they find that the organization is in violation of a given mandate, they **notify the Compliance/Legal and Executive teams in a final report**.

In the event a business is found to be non-compliant in any way, the organization will typically respond by:

- Acknowledging that they are aware of the non-compliance
- Determining a timeline to remediate the issue
- Develop a plan to bring the organization back into compliance

Audit Procedures

In this exercise, you'll review how *GeldCorp's* collects and stores user data to ensure their processes are GDPR compliant. In addition, you'll identify any data that must be protected according to PCI standards.

If you identify any incidents of non-compliance, you'll document a way for the organization to bring itself in line with regulation.

Suggested Time:
15 minutes

Contingency Planning for

Business Continuity

and

Disaster Recovery

Preparing for Breaches

Businesses engage in contingency planning to "plan for the worst"

A breach can have one of two results:

- **Mild/Moderate Breach:** The business has been impacted, but can still handle day-to-day operations at greater cost.
- **Serious/Catastrophic Breach:** The business has been impacted so severely they cannot operate. Instead, they must use their resources to contain the incident, recover from the disaster, and eventually return to operation.

BCP/DR Plans Typically Involve the Following:

- **Points and Modes of Failure:** Places where security is weak, or points of failure in a system like a network.

- **Projected Damages:** How a business will be affected in the event a given threat is realized.

- **Continuity/Recovery Plan:** For BCP, how the business could "patch" a mild/moderate incident to maintain operations during. For DR, explain how the business should prioritize its resources to recover from the reputational and operational damage of a catastrophic loss.

These plans will be different for every business.

Take a Break!

Presentations

In this exercise, you'll work in groups to develop BCP and DR plans for *Geldcorp*. You'll work with a group of consultants, and each group will develop a plan for a different domain of the company.

In particular, you'll develop plans for one of the following realms:

- Physical Environment
- Personnel
- Network
- Technology
- Security

Suggested Time:
1hr 30 minutes

Presentation Time!