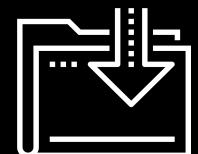




# Governance and Compliance

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 organization and  
the importance of security culture

DAY 2

Threat modeling and risk analysis

# Governance and Compliance

---

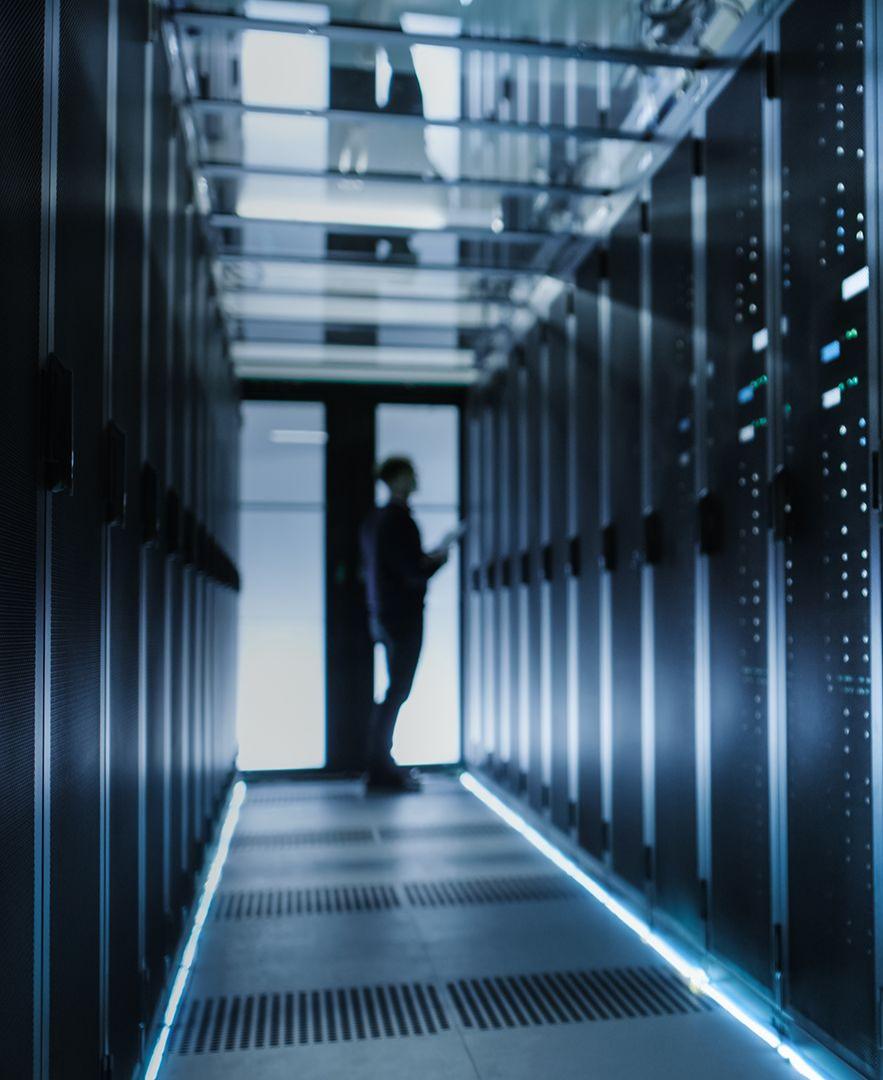
Today we will cover governance, compliance, and business continuity planning and disaster recovery (BCP/DR).

## Governance

*Codifying and enforcing proper behavior and operations.* That is, establishing standards of “right” and “wrong,” and enforcing those standards.

## Compliance

Enforcing the policies in order to meet those standards.

A photograph of a server room. In the foreground, a person is seen from behind, standing in a narrow aisle between two rows of server racks. They are looking at a screen, possibly a monitor or a tablet. The server racks are dark and have many small lights on them. The floor has blue glowing lines. The background is blurred.

Knowledge of governance, compliance, and BCP/DR is crucial context for all security professionals.

**Most professional security work is mandated by governance policies and subject to compliance audits.**

# Class Breakdown

---

Today's class will cover the following topics:

01

Codifying Rules with Policy and Procedures

02

Using Governance Frameworks to Guide Policy Decisions

03

Audit and Compliance

04

Business Continuity Planning and Disaster Recovery (BCP/DR)

05

Developing BCP/DR Recommendations for an Organization

# Codifying Rules with Policy and Procedures

## REVIEW

We began this week by developing a training plan to improve GeldCorp's security culture by changing employee behavior.

# Policy and Framework

---

A **policy** is a rule that defines the “right” behavior.

- ▶ Policies inform standards for behavior and operations.

A **governance framework** is a set of guidelines for the policies an organization should have in place.

- ▶ Governance frameworks describe the guarantees that a company must provide in order to remain compliant with federal regulations and industry standards.



# Policy and Framework

---

Today, we'll explore these concepts by:

Defining formal policies for the financial tech company GeldCorp.

Assessing what user data collected by GeldCorp is subject to General Data Protection Regulation (GDPR) and Payment Card Industry (PCI) Security Standard.

Determining whether GeldCorp's data collection practices are GDPR and PCI compliant.

# Using Organizational Goals to Define Policies

---

**Remember:** We developed training plans by *setting goals and determining the steps necessary to achieve them.*



The training plan prescribed a specific rule that employees should follow.  
For example, “Do not click on links from emails outside of the corporate intranet.”



This rule is an example of a **policy**—a course or principle of action proposed by a business.  
In this case the rule specified 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 a *policy* as a means of achieving a *goal*.

# How Business Goals Drive Policy Implementation

Business goals often drives policy creation. The two main types of business goals are:

## Internal/Volitional

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.

## External/Imposed

Targets that the business must hit because they will suffer consequences if they do not.

Examples include the requirement that online merchants process all credit card transactions securely, or suffer legal penalties if a customer's PII is breached.



# Internal Objectives and Policy: Example

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

An organization would hand this off to 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.



# Internal Objectives and Policy

Implementing a strong 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



Required monthly updates

# This policy defines clear standards of behavior.

- Administrators must follow very specific rules with regard to their passwords. Their computers will also enforce these rules.
- These rules are 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.



## Activity: Documenting Company Policies

In the previous lesson, you performed a risk analysis to help GeldCorp understand its most prominent threats. They've since used your results to set a number of internal security goals.

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

**Suggested Time:**  
**15 minutes**





**Times Up! Let's Review.**

# Using Governance Frameworks to Guide Policy Decisions

# Internal Objectives and Policy

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

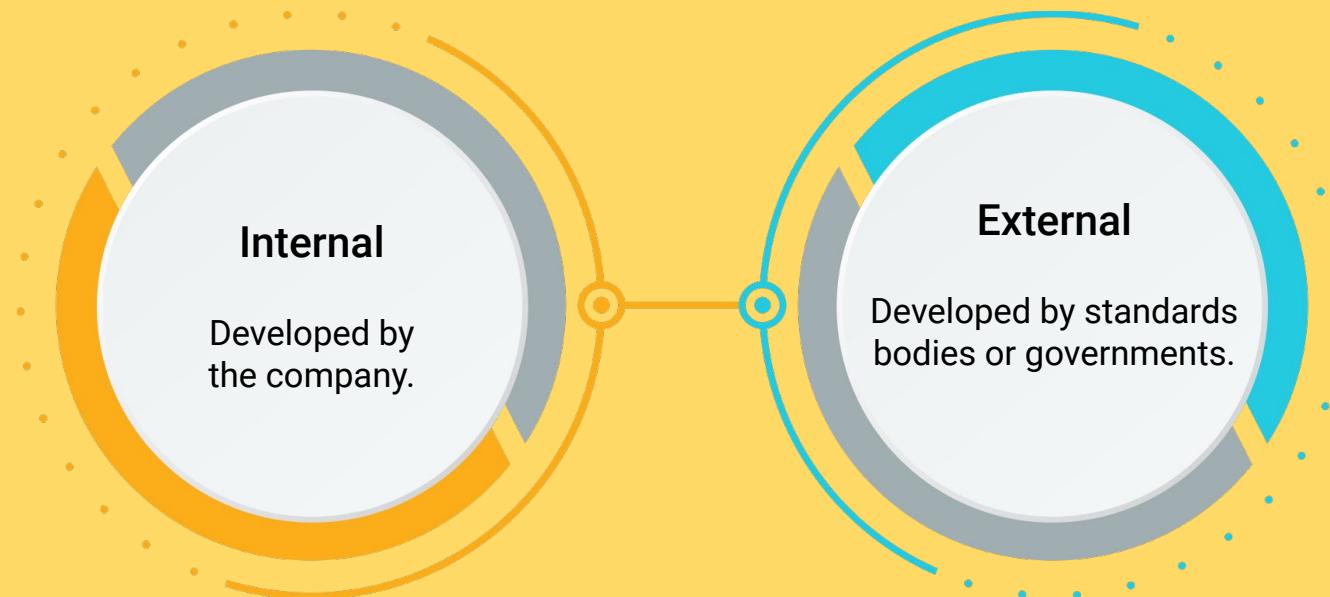


**Example:** Merchants that process financial transactions are legally required to guarantee their customers' data remains confidential. If a company suffers a breach resulting in the disclosure of customer PII, they may be fined and face other legal penalties.

# Governance Frameworks

---

There are some rules and policies that must be followed by everyone within an organization or industry. Collections of such policies are called **governance frameworks**. These can be:



SEC

- Frameworks originate from the **Securities and Exchange Commission (SEC)**, the regulatory organization in charge of proposing and enforcing laws regarding financial instruments (for example, stocks, bonds, options), and protecting consumers from fraud.
  - During the 1990s, the SEC worked with Congress to pass anti-fraud laws to discourage cybercrime.
  - In 2000, the SEC moved past simple anti-fraud laws by adopting the regulatory statute Regulation S-P.



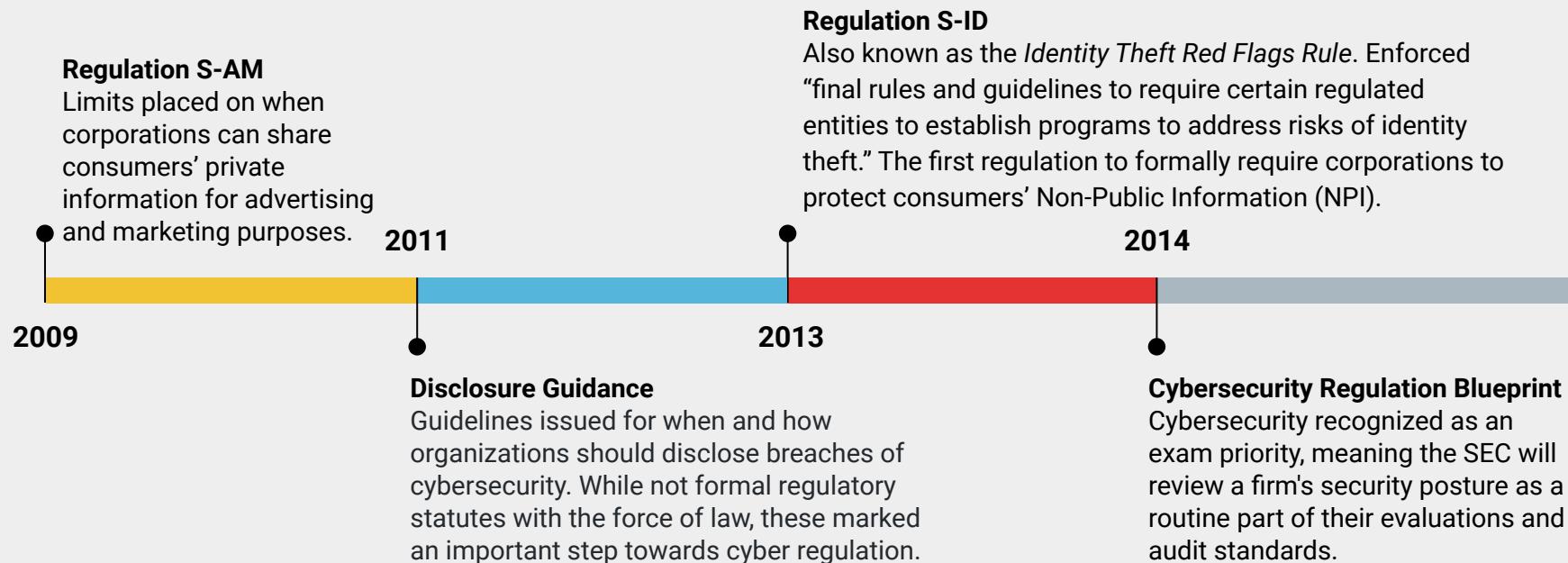
# Rule 30 of Regulation S-P (Safeguard Rule)

Regulation S-P did not focus entirely on security, but Rule 30 mandated that organizations establish written policies and procedures designed to:



# SEC Regulations

Additional regulatory statutes and administrative milestones followed in subsequent years.



# Common Governance Frameworks

All security professionals must be familiar with the following frameworks:



# Health Insurance Portability and Accountability Act (HIPAA)

**Title II: HIPAA Administrative Specification** is a provision establishing privacy standards around electronic access to healthcare data. Organizations must uphold the following standards to remain HIPAA compliant:



**National Provider Identifier Standard:** Requires all healthcare entities (people, healthcare providers, health plans, and employers) to have an ID, called the National Provider Identifier (NID).



**Transactions and Code Set Standard:** Standardizes health insurance claims.



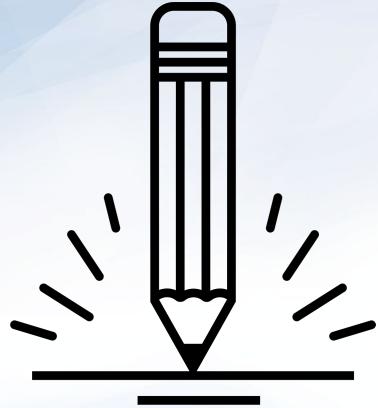
**HIPAA Privacy Rule:** Standardizes protections for individually identifiable health information, such as prescription information and lab results. This defines what data to protect.



**HIPAA Security Rule:** Standardizes measures of patient data security. This defines how well data should be protected.



**HIPAA Enforcement Rule:** Provides guidelines for investigating non-compliant providers.



## Activity: GDPR and PCI Compliance

In this activity, you'll explore the GDPR and PCI compliance framework and determine which data managed by GeldCorp is subject to their regulations.

**Suggested Time:**  
**15 minutes**





**Times Up! Let's Review.**



Countdown timer

15:00

(with alarm)

Break



# Audit and Compliance

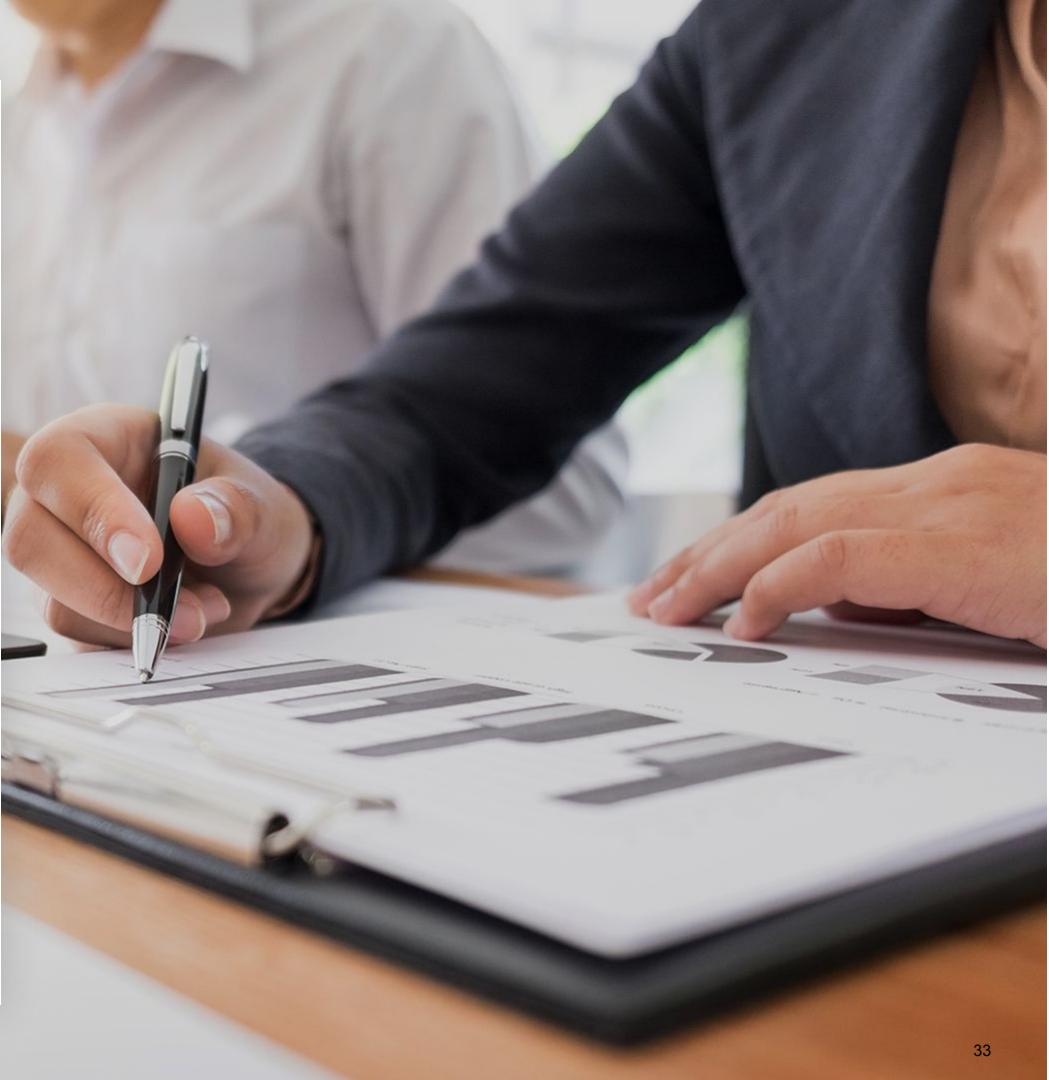
# Compliance and Audit

---

Businesses must enforce policies in order to guarantee **compliance** with regulations.

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

- Audits are typically run to make sure an organization is upholding the statutes required by government frameworks.



# Performing an Audit

---

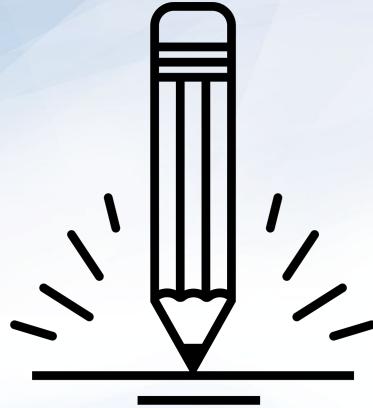
Auditors refer to each rule in the framework, and check that the business is following it.

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 fix the issue.
-  Developing a plan to bring the organization back into compliance.





## Activity: Audit Procedures

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

Document any incidents of non-compliance so the organization can fix the issues.

**Suggested Time:**  
**10 minutes**



# Business Continuity Planning and Disaster Recovery (BCP/DR)

All the machinery of governance and compliance can't guarantee that an organization will not experience a breach.

Businesses must still have contingency plans to prepare for the worst.

# Contingency Planning for Business Continuity

---

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 that they cannot operate.

Instead, they must use their resources to *contain* the incident, *recover* from the disaster, and eventually *return* to operation.



# Contingency Planning for Business Continuity

**Business continuity planning** (BCP) and **disaster recovery** (DR) planning focus on contingency plans in the event of a disruption or disaster, and ensure that the business can resume daily operations.

What are some possible disruptions or disasters?



Cyber attacks



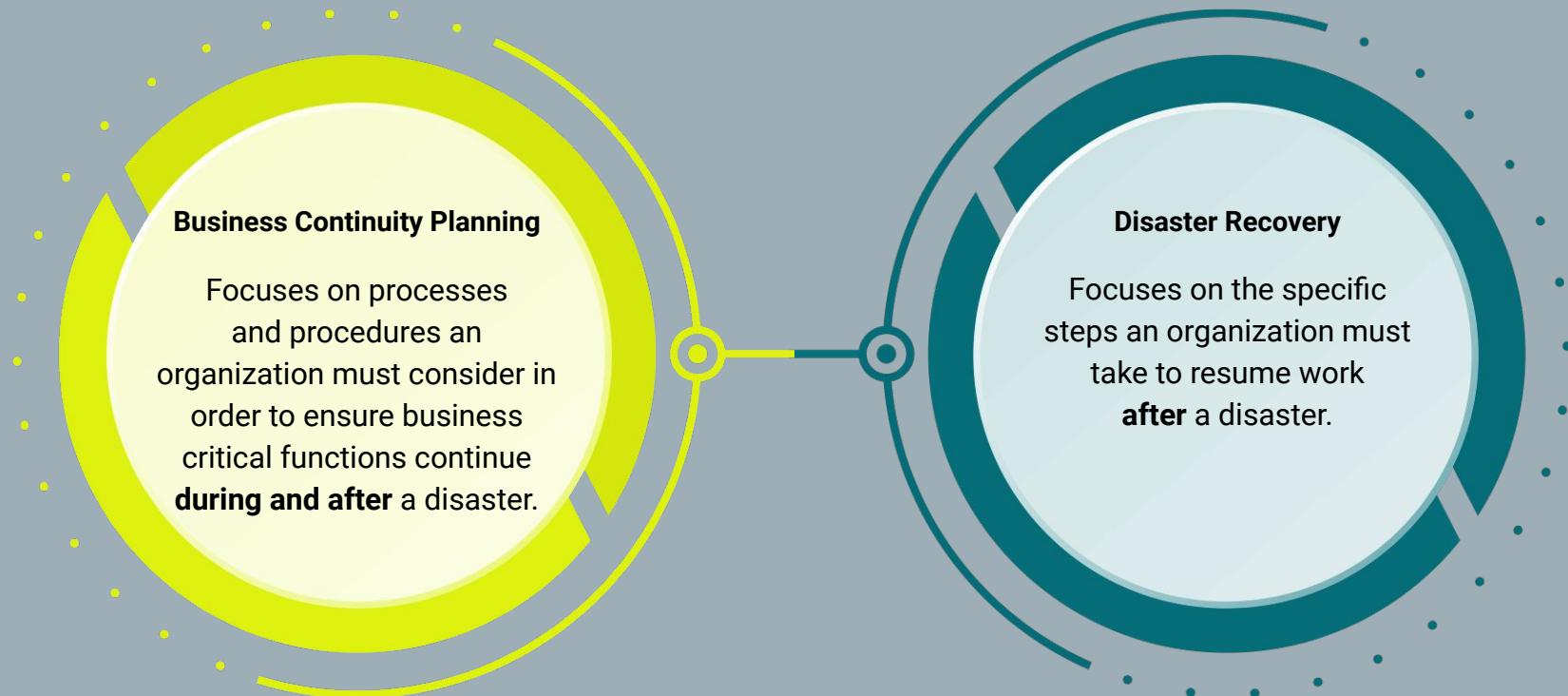
Human errors



Environmental disasters

# Business Continuity Planning vs. Disaster Recovery

It is important to note the differences between BCP and DR.



# Business Continuity Planning and Disaster Recovery

BCP and DR both begin with a contingency planning policy and business impact analysis.



Contingency planning focuses mainly on the availability of information systems, taking into account the impact of the company *not* having access to these systems.



Strategies for high-impact loss should consider high availability and redundancy options. For example, fully redundant load balanced systems at alternate sites, data mirroring, and offsite database replication.



High-availability options are normally expensive to set up, operate, and maintain and should be considered only for those high-impact information systems categorized with a high-availability security objective.



Lower-impact information systems may be able to use less expensive contingency options and tolerate longer downtimes for recovery or restoration of data.

# NIST Impact levels

---

The following descriptions of impact levels originally appear in NISTs *Contingency Planning Guide for Federal Information Systems*.

## Low

The loss of confidentiality, integrity or availability could be expected to have a **limited** adverse effect on organizational operations, assets and individuals.

## Moderate

The loss of confidentiality, integrity or availability could be expected to have a **serious** adverse effect on organizational operations, assets and individuals.

## High

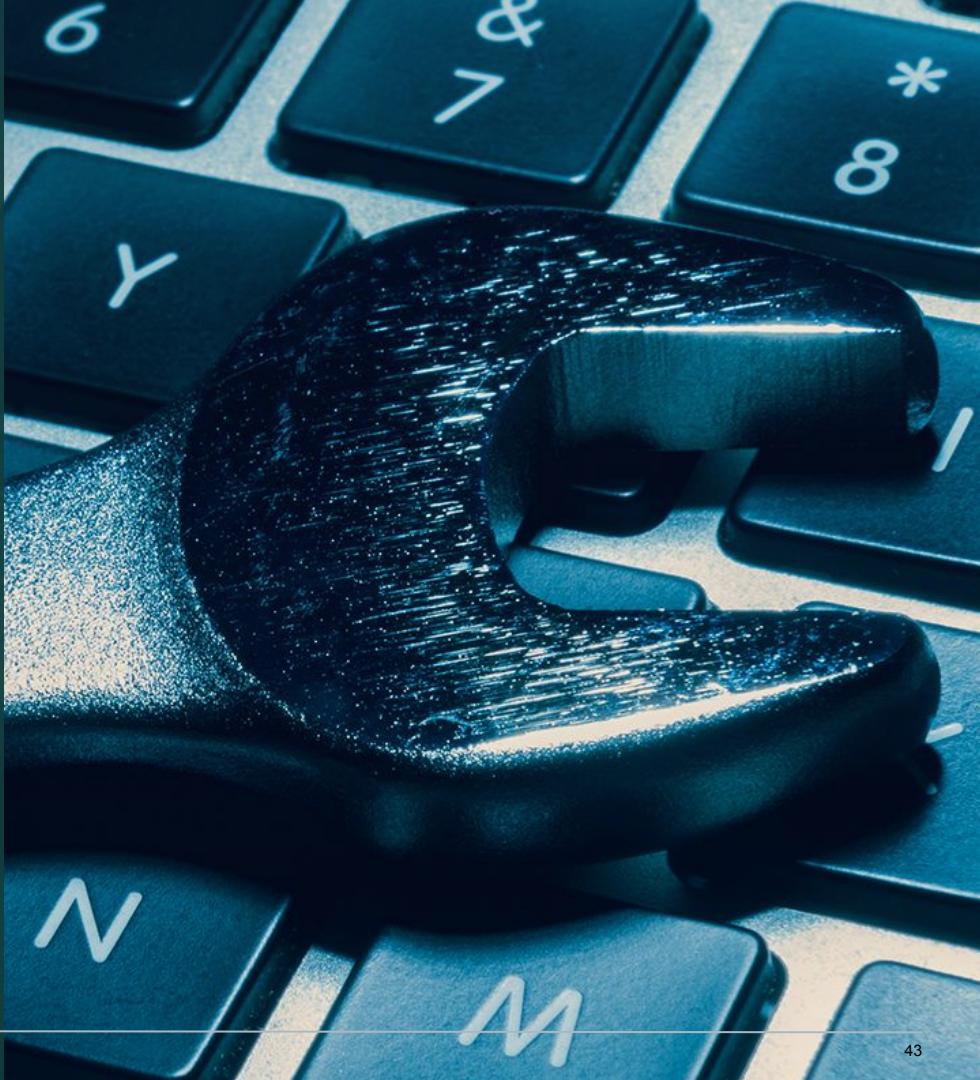
The loss of confidentiality, integrity or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, assets and individuals.

# Contingency Planning

---

Contingency planning results in a **contingency policy statement**, which establishes the organization's framework and responsibilities for maintaining confidentiality, integrity, and availability of data. It includes:

- Responsibilities of an emergency response team
- Resource requirements
- Training requirements
- Schedule for plan maintenance



# Business Impact Analysis and Risk Assessment

A pivotal step in BCP and DR planning is the Business Impact Analysis and Risk Assessment. Goals include:

Identify key processes and functions of the business.

Establish a detailed list of requirements for business recovery.

Determine the resource requirements needed to resume key processes.

Evaluate impact on daily operations.

Develop priorities and classifications of business processes and functions.

Develop recovery time requirements.

Determine financial, operations, and legal impact of disruptions.

# BIA Metrics

The results of the BIA impacts how the DR plan develops. In particular, it accounts for the following metrics:

**Recovery Point Objective (RPO)** represents the amount of data that a mission/business can afford to lose/recover (given the most recent backup copy of the data) after a disruption or system outage.

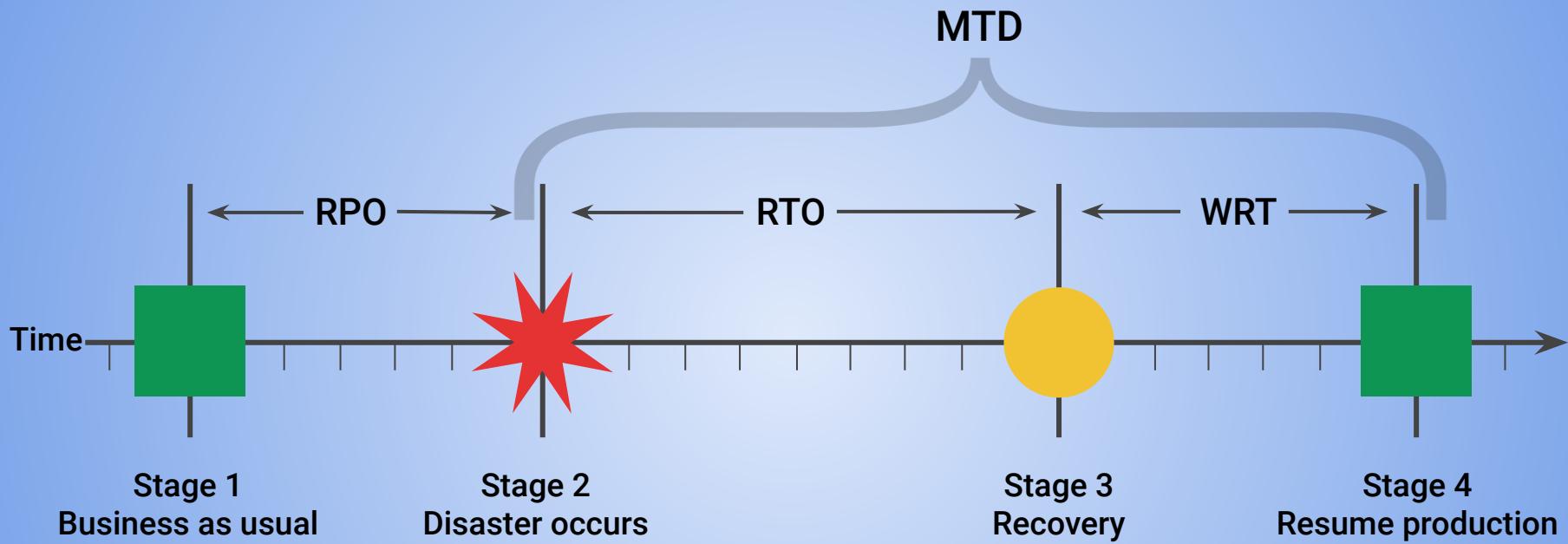
 For example, if a company performs weekly backups, they can tolerate/recover from a week's loss of data.

**Maximum Tolerable Downtime (MTD)** is the total amount of time a system can afford to be unavailable for users and the business.

 **Recovery Time Objective (RTO)** is the maximum tolerable amount of time needed to bring all critical systems back online after a disaster has occurred.

 **Work Recovery Time (WRT)** is the time available to get the systems working again. WRT is the remainder of the MTD after the RTO. If MTD is four days and RTO is one day, WRT is three days.

# BIA Metrics



# Alternate Site

One last consideration for disaster recovery is the use of **alternate sites** to house critical data technology functions. While rare, disasters may require that these operations be moved to one an alternate sites.



A **hot site** is ready to go at all times. It has equipment loaded with currently available data and can immediately continue operations. It is costly, but important for mission-critical data.



A **cold site** has very little set up. It is typically not used until after a disaster, and needs a strategy for rapid setup.



A **warm site** is in-between. For example, servers, hardware, software, and other equipment might be setup but not loaded with the latest data.



## Activity: Disaster Recovery Planning

In this activity, you will continue to work in groups to create a high level disaster recovery plan for GeldCorp.

Suggested Time:  
10 minutes





**Times Up! Let's Review.**