Governance and Compliance

Cybersecurity

GRC 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 business continuity planning and disaster recovery ensure business and mission critical functions in the event of a disruption.

Structure of the security organization and the importance of security culture.

Threat modeling and risk analysis.

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

Governance:
codifying and enforcing proper behavior and operations by establishing standards of “right” and “wrong”.

Compliance:
enforcing the policies in order to meet those standards.

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


Recap


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

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.

Policy and Framework

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 in emails leading outside 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 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 a policy as a means of achieving a goal.

Policy and Framework

policy	A rule that defines the “right” behavior.
governance framework	Defines the policies an organization must have in place.

Policies inform standards for behavior and operations.

Organizations must use these frameworks to remain compliant with federal regulations and industry standards.

Business Goals and Policy Implementation

Business goals often drive 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.

For example:
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

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

One possible implementation:

Require all domain administrators to use strong passwords, and require 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 for 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:

- CloGyPTioNEntEDist5$
- coffee&Donuts975
- 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 require 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 this activity, you will develop and document policies to help Geldcorp address its most critical threats.

Suggested Time:

20 Minutes

Time’s Up! Let’s Review.

Questions?

Managing Risk in IT Organizations

External Objectives and Policy

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

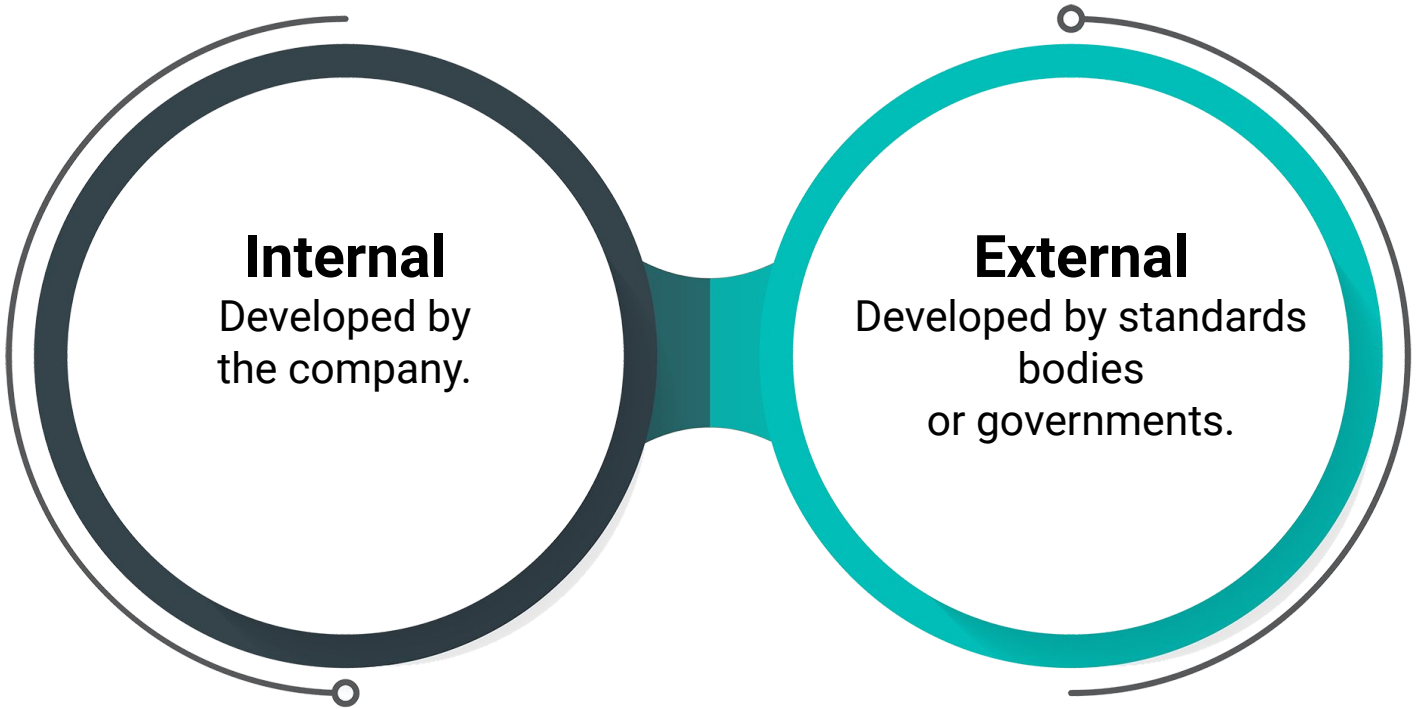
Example:

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 are rules and policies that must be followed by everyone in an organization or industry.

Governance Frameworks



Governance Frameworks

As information security professionals, it is important to understand the distinctions between:

- Laws
- Regulations
- Policies
- Guidelines
- Frameworks

All of these will help guide your decision-making process in everything you do.

A **policy** is a set of rules that inform standards for behavior and operations.

Policy Examples

Bring Your Own Device (BYOD)

- A form of non-intrusive policy adopted by organizations that specifically define the acceptable use of non-company owned devices.
- Devices referenced in this policy may include desktop computers, routers, switches, test measurement equipment, and weather equipment.

Mobile Device Management (MDM)

- An example of a restrictive or intrusive policy that is a subset of a BYOD policy.
- MDM is more specifically defined as an acceptable use policy of personally-owned mobile devices. Devices referenced in this policy include cell phones, laptops, and WiFi hotspots.

Guidelines are similar to policies, as they are issued by organizations to make the actions of its employees or departments more predictable, and presumably of higher quality.

Guidelines are not mandatory.
They are only suggestions, meant to be followed by those to which they apply.

Laws are policies that are written in legal language, and voted upon and passed by legislative bodies of government.

Laws are enforced by agencies tasked with overseeing and monitoring the rule of law.

One such organization is the **Security and Exchange Commission (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.

SEC

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.

https://www.sec.gov

Industry-Specific Laws

Different industries have different laws:

The Family Educational Rights and Privacy Act (FERPA)	**Gramm-Leach-Bliley Act (GLBA)**	**Federal Information Security Management Act of 2002 (FISMA)**	**Health Insurance Portability and Accountability Act (HIPAA)**
Protects the privacy of student education records. Parents or eligible students have the right to request records be corrected if they believe them to be misleading or inaccurate.	Requires financial institutions that provide consumers financial products and services to provide an explanation of their information-sharing practices to safeguard sensitive data.	Requires the protection of government data, operations, and assets against natural or man-made threats.	Regulates the flow of healthcare information and states how personally identifiable information (PII) should be protected from misuse and theft within the healthcare industry.

Regulations are detailed instructions on how laws should be enforced.

Sometimes referred to as **administrative laws**, regulations are backed by the force of law and their application is mandatory.

Legislative bodies pass laws and government agencies create regulations that implement the laws.

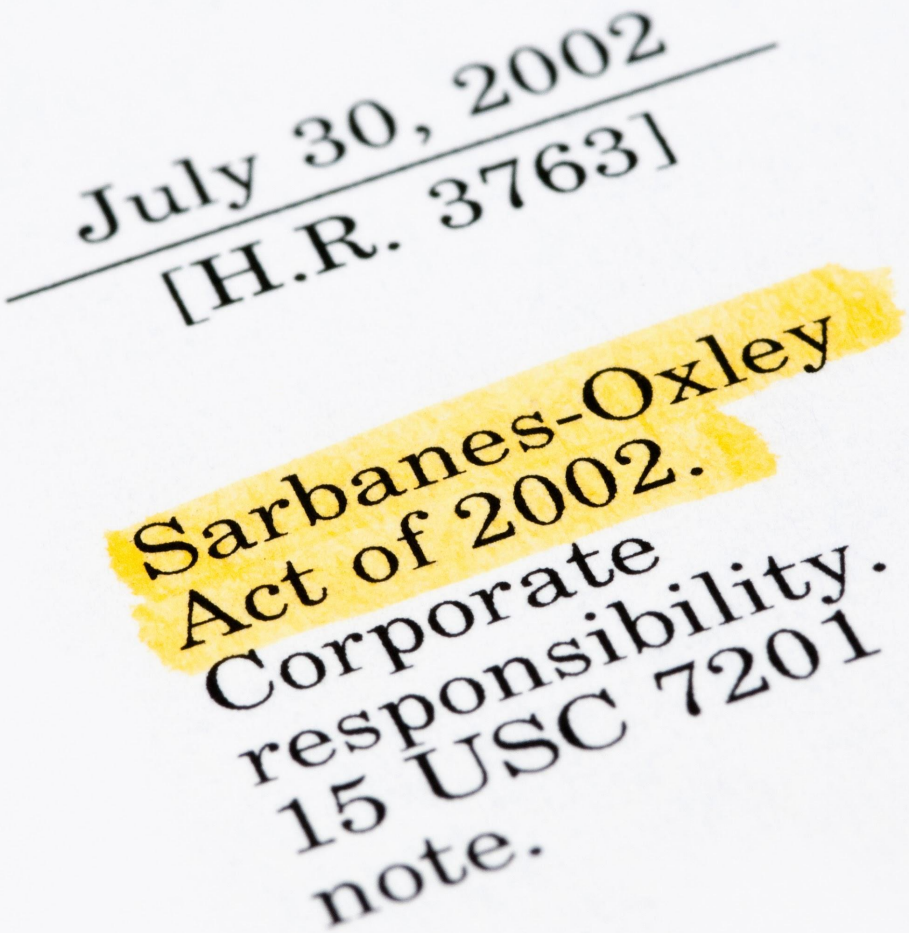
Regulations

Some of the more popular regulations within information security include:

Sarbanes Oxley (SOX), a result of the Enron and WorldCom scandal, holds corporate officers, board members, and executive management liable if the organization they represent is not compliant with the law.

Noncompliance includes negligence and failure to implement any recommended precautions.

Due diligence and **due care** must be demonstrated at all times.



Regulations

Some of the more popular regulations within information security include:

General Data Protection Regulation (GDPR) protects the private data of all citizens of the European Union (EU) and European Economic Area (EEA).

- Requires 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.

Standards are published specifications used to establish a common language and technical criteria across an organization or industry.

Standards Example

Merchants that process financial transactions are contractually required to comply with the **Payment Card Industry Data Security Standard (PCI-DSS)** to guarantee that their customers' data remains confidential.

If a company suffers a breach that results in the disclosure of customer PII, they may have to pay large fines and face other legal penalties.

Risk Management Frameworks

Properly implemented information security frameworks allow security professionals to intelligently manage cyber risks within their organizations.

- Frameworks consist of various documents clearly defining adopted procedure, policies, and processes, which an organization must follow.
- Having an information security framework reduces an organization's risk and exposure to vulnerabilities.

Risk Management Frameworks

Establishing a solid information security framework provides many advantages:

01

Instills confidence in your industry.

02

Establishes a strong reputation with business partners.

03

Provides a reputable relationship with customers.

A **risk management framework (RMF)** is a set of standards developed by the National Institute of Standards and Technology (NIST).

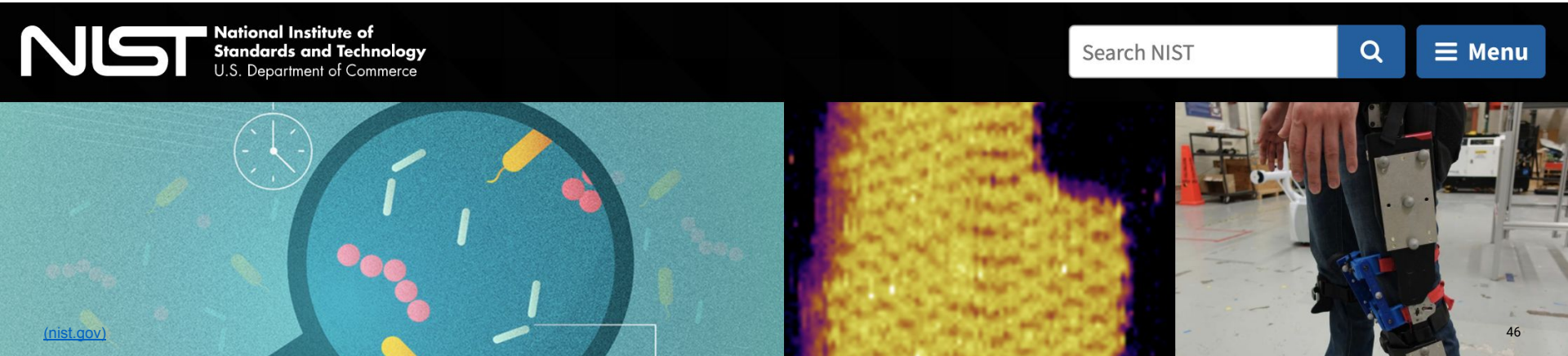
Risk Management Frameworks

Special Publication 800-37r2

"Risk Management Framework for Information Systems and Organizations," describes the formal RMF certification and accreditation process.

Special Publication 800-53

"Security and Privacy Controls for Federal Information Systems and Organizations," describes a structured process for an organization to select system security controls and integrate them as part of an organizational risk management program.



National Institute of Standards and Technology (NIST)

NIST is a federal agency within the United States Department of Commerce.

- NIST's mission is to develop and promote standards, measurements, and technology that enhances productivity, facilitates trade, and improves quality of life.
- Since 2014, the NIST Cybersecurity Framework has provided guidance for critical infrastructure so organizations can better manage and reduce cybersecurity risks.

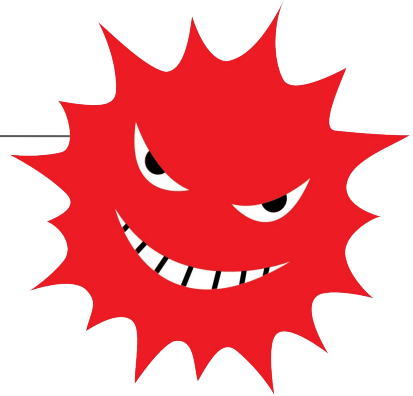
NIST Cybersecurity Framework

The NIST Cybersecurity framework is made of Categories, Subcategories, and Informative Resources.

Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Detect			
Respond			
Recover			

Let’s take a look at how an organization would implement the NIST Risk Management Framework.

NIST RMF Scenario



An organization has just recovered from an attack.
They must now consider what can they can do to mitigate this attack from happening again.

Solution

The organization decides to incorporate “lessons learned” as part of their incident response. They will adopt and incorporate a security control from the Improvements category of the NIST RMF with a subcategory of **RS.IM-1**.

Function	Category	Subcategory	CCS CSC	COBIT 5	ISA 62443-2-1: 2009	ISA 62443-3-3: 2013	ISO/IEC 27001:2013	NIST SP 800-53 REV. 4
RS	IM	IM-1		BA101.13	4.3.4.5.10, 4.4.3.4		A.16.1.6	CP-2, IR-4, IR-8

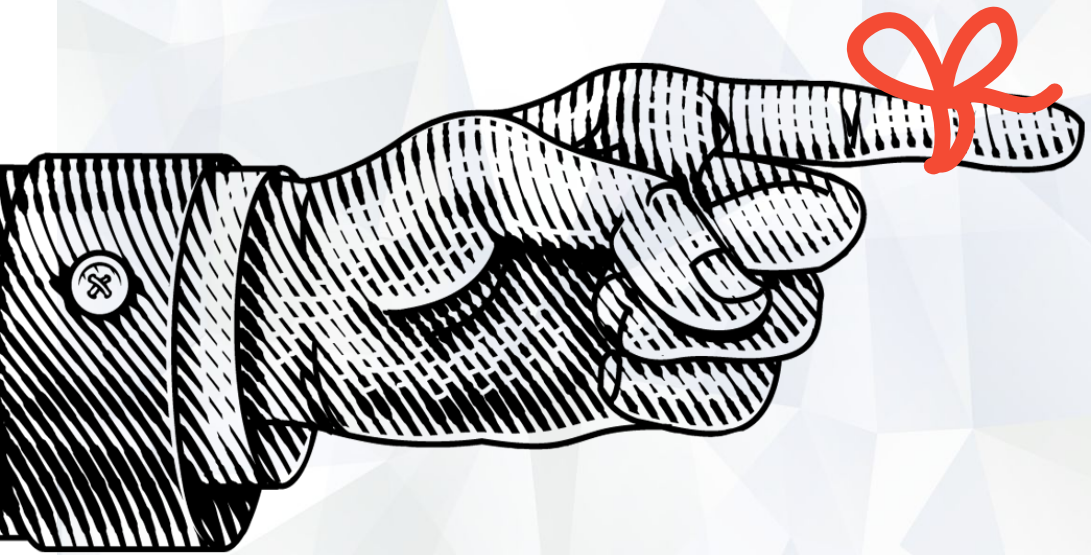
Appendix A - Framework Core Informative References

NIST RMF Scenario

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RS.IM-1: Response plans incorporate lessons learned.

Function	Category	Subcategory	Informative Resources
Respond	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/ response activities.	**RS.IM-1**: Response plans incorporate lessons learned	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8



Remember,

An RMF is a set of documents that define best practices.

An organization may voluntarily follow these to efficiently manage its cybersecurity risks.

Setup for Next Activity

In the next activity, you will play the role of a security consultant for a new online auction company, **E-Auctions.com**.

- You are tasked with determining E-Auctions.com's security posture before they launch their business.
- You'll accomplish this by conducting an interview with the CEO of E-Auctions.com. **Your instructor will play the role of CEO.**
- As a class, you will each develop one question about E-Auctions.com's security posture and take turns interviewing the CEO.

Setup for Next Activity

You will be assigned a number between 1 and 22.

- This number will correspond to a NIST category.
- You will develop a question relevant to the NIST category you are assigned.
- NIST documentation is provided so you can learn about your category and subcategories.

1	Asset Management (ID.AM)
2	Business Environment (ID.BE)
3	Governance (ID.GV)
4	Risk Assessment (ID.RA)
5	Risk Management Strategy (ID.RM)
6	Access Control (PR.AC)
7	Awareness and Training (PR.AT)
8	Data Security (PR.DS)
9	Information Protection Processes and Procedures (PR.IP)
10	Maintenance (PR.MA)
11	Protective Technology (PR.PT)

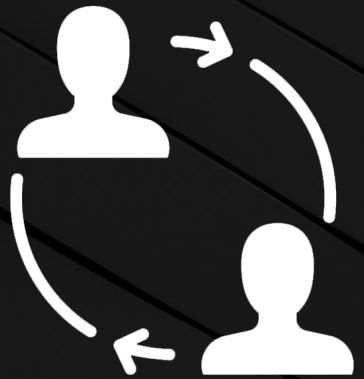
12	Anomalies and Events (DE.AE)
13	Security Continuous Monitoring (DE.CM)
14	Detection Processes (DE.DP)
15	Response Planning (RS.RP)
16	Communications (RS.CO)
17	Analysis (RS.AN)
18	Mitigation (RS.MI)
19	Improvements (RS.IM)
20	Recovery Planning (RC.RP)
21	Improvements (RC.IM)
22	Communications (RC.CO)

Activity: CEO Interviews

In this activity, you will formulate a question and pose it to the CEO of E-Auctions.com.

Suggested Time:

10 Minutes



Everyone Do: CEO Interview

Take turns asking your questions.

Suggested Time:

25 Mins

Questions?

Countdown timer

15:00

(with alarm)

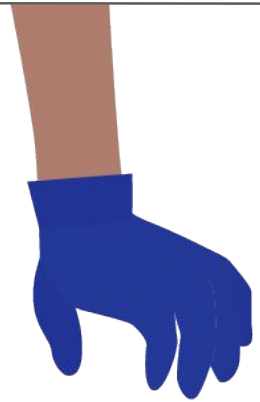
Business Continuity Planning and Disaster Recovery (BCP/DR)

All of 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:



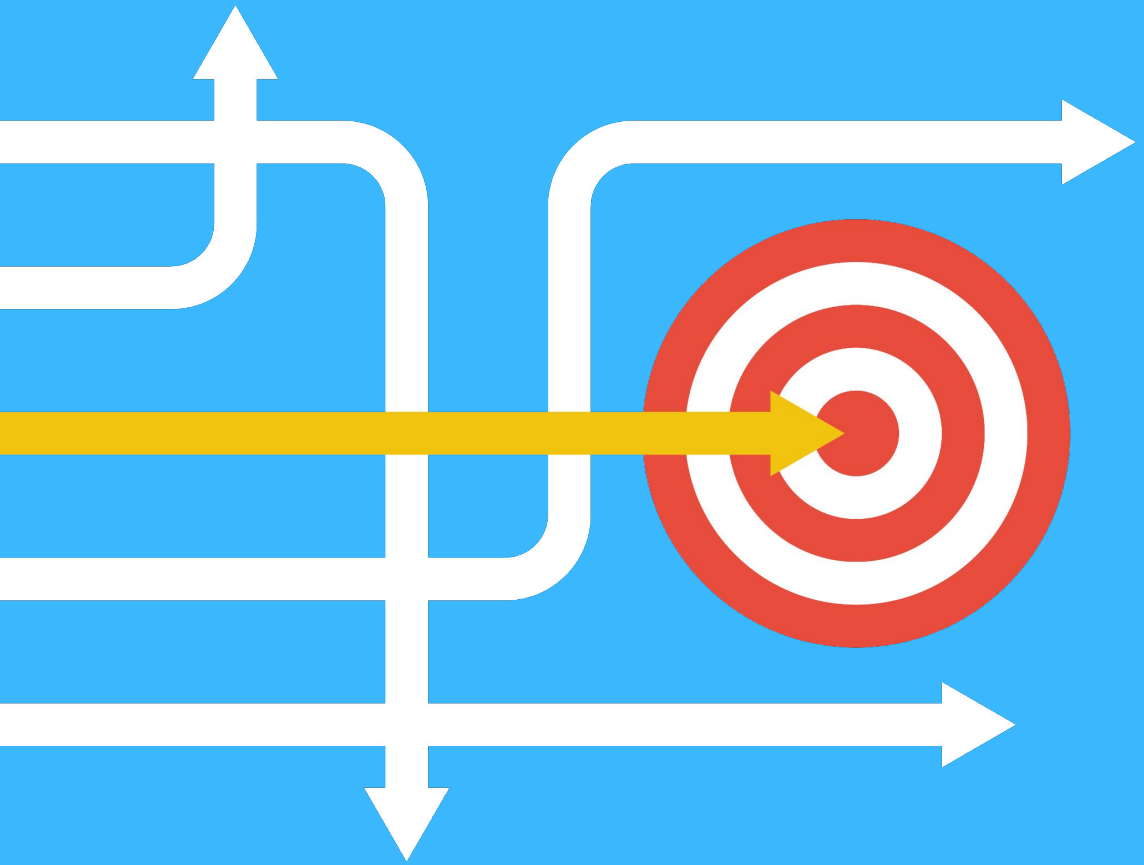
01 **Mild / moderate breach:**

The business has been impacted, but can still handle day-to-day operations at greater cost.

02 **Serious / catastrophic breach:**

The business has been impacted so severely that it cannot operate. Instead, they must use their resources to *contain* the incident, *recover* from the disaster, and eventually *return* to operations.

Security Concerns vs. Business Concerns



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?

Contingency Planning for Business Continuity

Cyberattacks

Human errors

Environmental disasters

Business Continuity Planning vs. Disaster Recovery

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

Business Continuity Planning

Focuses on processes and procedures to ensure business critical functions continue **during and after** a disaster.

Disaster Recovery

Focuses on the specific steps an organization must take to resume work **after** a disaster.

Business Continuity Planning and Disaster Recovery

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

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

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

Contingency Planning

A contingency policy statement includes:

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

Business Impact Analysis (BIA) and Risk Assessment

A critical step in BCP and DR planning is 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 informs the following metrics:

Recovery Point Objective (RPO):

Amount of data that a 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.

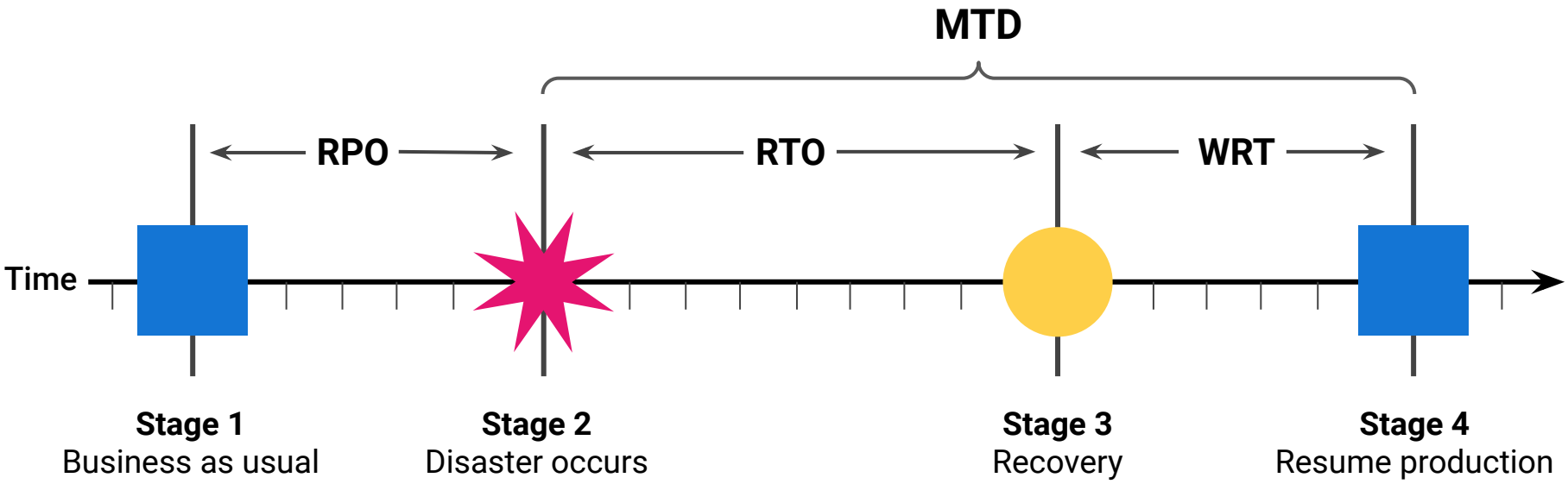
Maximum Tolerable Downtime (MTD):

Total amount of time a system can afford to be unavailable for users and the business.

Recovery Time Objective (RTO): Maximum tolerable amount of time needed to bring all critical systems back online after a disaster occurs.

Work Recovery Time (WRT): 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


MTD
RPO
RTO
WRT
Time
Stage 1
Business as usual
Stage 2
Disaster occurs
Stage 3
Recovery
Stage 4
Resume production

Alternate Sites

One last consideration for disaster recovery is the use of **alternate sites** to house critical data technology functions. While disasters are rare, they may require that operations move to an alternate site.

A **hot site** is ready 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 existing infrastructure.

It is not typically used until after a disaster occurs, so there must be a strategy for setting it up quickly when the time comes.

A **warm site** is in-between.

For example, servers, hardware, software, and other equipment might be set up 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

Time’s Up! Let’s Review.

Questions?


The End