Today's class will introduce you to governance, compliance, and business continuity planning and disaster recovery.

* **Governance** is concerned with codifying and enforcing proper behaviour and operations. Governance is the field in which standards of "right" and "wrong" are established and enforced.
* **Compliance** is about enforcing the policies necessary to meet those standards.

Knowledge of governance, compliance, and BCP/DR is crucial for all security professionals. Most of what security professionals do is mandated by governance policies and subject to compliance audits.

Today's class will cover the following topics:

* Codifying Rules with Policy and Procedures
* Using Governance Frameworks to Guide Policy Decisions
* Risk Management within an IT Organization.
* Business Continuity Planning and Disaster Recovery
* Describing BCP/DR Recommendations for an Organization

02. **Codifying and Enforcing Behaviour with Policies and Procedures**

The week began by developing a training plan to improve *GeldCorp's* security culture. This training plan was meant to protect the organization by changing employee behaviour.

* The training exercise defined what employees *should* do when faced with suspicious links. In other words, it defined the "right" behaviour.

A rule that defines the "right" behaviour is called a **policy**. Organizations use policies to define standards for behaviour and operations.

* Each individual policy is just one rule. In practice, organizations will have many policies, and therefore many rules, 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 what a company must do to remain compliant with federal regulations and industry standards.

Today, we'll explore these concepts by:

* Defining formal policies for GeldCorp.
* Assessing what user data collected by GeldCorp is subject to GDPR and PCI.
* Determining whether GeldCorp's data collection practices are GDPR and PCI compliant.

Using Organizational Goals to Define Policies

You developed your training plan by setting a goal and determining the necessary steps to achieve it.

* The training plan prescribed a specific rule that employees should follow. For example: "Do *not* click on links to domains outside of the corporate intranet."
* This rule is an example of a policy, which is a course 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 five percent. In other words, the business implemented policy as a means of achieving this goal.

Such business goals often drive the development of policies. There are two general categories of business goals:

* **Internal/Volitional**: Targets that the business sets in its own interest. For example, an organization might aim to reduce long-term security expenses to be less than $400,000.
* **External/Imposed**: These are targets that the business must hit because they will suffer consequences if they do not. Examples include requiring e-merchants to handle all credit card transactions securely or face legal consequences if they experience a breach of customer PII (personally identifiable information).

Internal Objectives and Policies

Suppose we want to reduce unauthorized root-level login incidents on domain controllers to zero:

* An organization that adopts such a policy would hand it 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.
* A password policy might require that administrators create passwords with:
  + At least 16 characters.
  + At least one letter and one number.
  + At least one special character (', (, ], etc.).
* Additionally, the password policy could require that passwords do not contain any portion of the administrator's username, and that new, strong passwords are created every month.

This policy defines clear standards of behaviour:

* Administrators are expected to follow very specific rules when creating passwords, which their computers will enforce.
* And these rules are specifically designed to achieve the goal of reducing the incidence of unauthorized root-level logins on domain controllers to zero.

Below is an example of a completed password policy:

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.

**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`

**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.

* This policy still does not guarantee strong passwords:

For example, n0tparticularly!strong is legal, but easy to crack. It is up to policy developers to determine whether a policy is secure enough.

**Managing Risk in IT Organizations**

Internal policies often support business goals, such as guaranteeing 99% uptime.

* However, businesses often must follow rules that they don't necessarily set for themselves.
* Such rules may not directly benefit the business, but rather, may be mandated by regulations, laws, or industry standards.

As information security professionals, it is important to understand the distinctions between **laws**, **regulations**, **policies**, **guidelines**, and **frameworks**. All of these will help guide your decision-making process in everything you do.

**Policies**

A policy is a set of ideas or plans that inform decision making within business, government, politics, or economics.

Examples of policies include:

* **Bring Your Own Device (BYOD)** is a non-intrusive policy adopted by organizations that specifically defines the acceptable use of non-company owned devices. Devices referenced in this policy may include personally owned devices such as desktop computers, routers, switches, test measurement equipment, and weather equipment.
* **Mobile Device Management (MDM)** is an example of a restrictive or intrusive policy that is a subset of a BYOD policy. MDM is an **acceptable use policy** related to personally owned mobile devices. Devices referenced in this policy include cell phones, laptops, and WiFi hotspots.

: question: Can anyone think of circumstances in which an organization would require a mobile device management policy?

* Answer: Any company that has a remote workforce.

**Guidelines**

A guideline is like a rule. Guidelines are issued by organizations to make the actions of its employees or departments more predictable and, presumably, higher quality.

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

**Laws**

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

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

* One such organization is the **Security and Exchange Commission** (**SEC**).
  + Governance frameworks codify standards that all businesses should follow.
  + In the United States, these frameworks come from statutes (laws passed by Congress) adopted by the SEC, the regulatory body in charge of enforcing and proposing laws about financial instruments (stocks, bonds, options, etc.), and protecting consumers from fraud.
  + In the 1990s, the internet grew explosively, leading to the emergence of cybercrime. During the 90s, the SEC worked with Congress to pass anti-fraud statutes to discourage cybercrime.
  + **Note:** An anti-fraud statute, in our context, is a law criminalizing the use of technology to commit fraud.
* Since businesses in different industries manage different kinds of data, they must meet these obligations in different ways. This is why there are different laws for different industries. You should be aware of some of these, including:
  + **The Family Educational Rights and Privacy Act (FERPA)** protects the privacy of student educational records. Parents or eligible students have the right to request that records be corrected if they believe they are misleading and/or inaccurate.
  + **Gramm-Leach-Bliley Act (GLBA)** requires financial institutions who provide consumers financial products and services to provide an explanation of their information-sharing practices to safeguard sensitive data.
  + **Federal Information Security Management Act of 2002 (FISMA)** defines the framework for protecting government data, operations, and assets against natural or man-made threats.
  + **Health Insurance Portability and Accountability Act (HIPAA)** regulates the flow of healthcare information and defines how personally identifiable information (PII) must be protected from misuse and theft within the healthcare industry.
    - Any organization that collects, stores, administers, or provides PII is obligated to abide by HIPPA. This includes such organizations as health maintenance organizations (HMOs), dental offices, optometrist practices, and chiropractic offices.

**Regulations**

Regulations are detailed instructions for how to enforce laws.

* Sometimes referred to as administrative laws, regulations are legally required, and their application is mandatory.
* Legislative bodies pass laws, and government agencies create regulations that implement the laws.

Note the difference between laws and regulations:

* Laws govern everyone equally.
* Regulations only affect organizations whose operations are directly enforced by the regulation, i.e., SOX and GDPR.

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 responsible if the organization they represent is not compliant with a law. Noncompliance includes negligence and failure to implement any recommended precautions. Due diligence and due care must be demonstrated at all times.
  + **Due diligence** is, for example, when a company or individual properly investigates all of the possible weaknesses and vulnerabilities, in order to fully understand threats.
  + **Due care** is, for example, when a company has done all it can reasonably do to prevent a security breach, compromise, or disaster, and implemented the necessary countermeasures, such as security controls (safeguards).
* **General Data Protection Regulation (GDPR)** protects the private data of all citizens of the European Union (EU) and European Economic Area (EEA). It requires organizations that process data belonging to EU citizens to 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.

You'll learn more about individual regulations on the job, but the ones that you need to know specifically depend on the industry you work in.

: question: What is the difference between a regulation and a law?

* Answer: Laws govern each person equally. Regulations affect organizations or entities whose operations, such as the protection of data, require specific vigilance.

**Standards**

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

* For example, merchants that process financial transactions are legally required to comply with the **Payment Card Industry Data Security Standard** (**PCI-DSS**) to help 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/or face other legal penalties.

**Risk Management Frameworks**

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

* The RMF is explicitly covered in the following NIST publications:
  + [Special Publication 800-37r2](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf), “Risk Management Framework for Information Systems and Organizations” describes the formal RMF certification and accreditation process.
  + [Special Publication 800-53](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf), “Security and Privacy Controls for Federal Information Systems and Organizations” describes a structured process for selecting system security controls and integrating them as part of an organizational risk management program.

A properly implemented information security framework allows security professionals to manage cyber risks more intelligently within their organizations.

* Frameworks consist of various documents that clearly define adopted procedures, policies, and processes followed by an organization.
* Having an information security framework in place reduces an organization's risk and exposure to vulnerabilities.

Other advantages of establishing a solid information security framework include:

* Installs confidence in your industry.
* Establishes a strong reputation with business partners.
* Provides a reputable relationship with customers.

**NIST produces one of the most used cybersecurity frameworks today.**

National Institute of Standards and Technology (NIST)

NIST is a federal agency in 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](https://www.nist.gov/cyberframework) has provided guidance for critical infrastructure so organizations can better manage and reduce cybersecurity risks.

At the core of the framework is a set of actions that enable specific outcomes. The framework core isn't a checklist, rather it provides a set of key cybersecurity outcomes to work towards.

The core of the framework includes four elements:

* **Functions:** Identify, Protect, Detect, Respond, and Recover. These functions aid in the expression of cybersecurity risk management by organizing information that enables risk management decisions. Functions also align with current methodologies for incident management.
* **Categories:** Subdivisions of functions. These are grouped cybersecurity outcomes that are closely related to specific needs and activities.
  + Examples include Detection Processes, Access Control, and Asset Management.
* **Subcategories:** Divides categories further into specific outcomes of specific activities. The results of of this subset lead to the achievement of outcomes within each category.
* **Informative References:** Specific sections of guidelines, standards, and practices that describe methods for achieving outcomes in each subcategory.

Next, we'll look at how an organization would implement the adoption of the NIST RMF.

* The image below contains a snippet of a security control category from the NIST RMF for response (RS) and recover (RC).
  + If an organization wanted to include any of these security controls in their local policies, they would adopt the use of the category and subcategory codes along with the associated language. It could be as easy as a copy and paste.
* For example: An organization has just recovered from an attack. The organization must now consider what they can do to mitigate this attack from happening again.
  + 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**.
    - **Improvements (**[**RS.IM**](http://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.
* An RMF is a set of documents that define best practices that an organization voluntarily follows to manage its cybersecurity risks most efficiently.
* RMFs are completely voluntary and designed to increase the resiliency of an organization’s defences.

: question: What are two advantages of implementing a risk management framework?

* Answer: Three examples are: installs confidence in your industry, establishes a strong reputation with business partners, and provides a reputable relationship with customers.

**Contingency Planning for Business Continuity and Disaster Recovery**

Even with all the measures put in place by governance and compliance, it's not guaranteed that an organization will not experience a breach. Therefore, businesses engage in contingency planning to "plan for the worst."

Organizations need to be ready for any disturbances that can lead to interruptions or completely stop their operations.

* We’ve discussed controls to mitigate threats, vulnerabilities, and risks. But organizations also simultaneously need to think on a larger scale about building an infrastructure that can minimize the impact on critical functions.
* Contingency planning not only considers technology and information systems, but also the larger business processes, employees, and facility requirements.

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 it cannot operate. Instead, it must use its resources to *contain* the incident, *recover* from the disaster, and eventually *return* to operation.

Business continuity planning (BCP) and disaster recovery (DR) planning produce contingency plans in case of a disruption or disaster and ensure that the business can get back on its feet and remain operational.

* Possible disasters include cyberattacks, human errors, and environmental disasters, such as earthquakes and fires.
* As it relates to the CIA triad, contingency planning is focused primarily on ensuring the availability of information, including timely and reliable access to it.

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

* Business continuity planning focus on processes and procedures that an organization needs to consider in order to ensure that critical functions continue both during and after a disaster.
  + Since this takes into consideration business processes, business continuity involves much more comprehensive and thorough planning to ensure an organization’s long-term success.
* Disaster recovery is more focused on the specific steps that a organization needs to take to resume work after a disaster. It is concerned more with the technology and information infrastructure and related complexities.
  + For example, some of the concerns for DR are how information systems and their operations can be moved to another location following an incident, how information is backed up, and the costs associated with equipment replacement.

**Contingency Planning**

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

* This description was taken from the [NIST Contingency Planning Guide for Federal Information Systems](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf):
  + Contingency planning considerations and strategies address the impact level of the availability security objective of information systems.
  + Strategies for high-impact information systems should consider high availability and redundancy options in their design. Options may include 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.

**The information below on impact levels was taken directly from the**[**NIST Contingency Planning Guide for Federal Information Systems**](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf):

* If the potential impact is **low**, the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
* If the potential impact is **moderate**, the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
* If the potential impact is **high**, the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Contingency planning should result in a **contingency policy statement**. This establishes the larger organizational framework and responsibilities related to maintaining confidentiality, integrity, and availability of data, and the impact level to those objectives in the event of a disruption.

* Additionally, a policy statement also considers roles and responsibilities of an emergency response team, resource requirements, training requirements such as exercise and testing schedules, and schedules for maintaining the plan.

**Business Impact Analysis**

The first step in BCP and DR planning is to conduct a **business impact analysis (BIA)** and risk assessment. We covered many aspects of risk analysis in the previous class.

* Conducting a BIA is a lengthy process and outside the scope of today's class. Typically, it is a multiphase process that involves gathering and evaluating information and preparing a report for senior management.
* The goals of BIA include:
  + Identify key processes and functions of the business.
  + Establish a detailed list of requirements for business recovery.
  + Determine what the resource interdependencies are.
  + Determine the impact on daily operations.
  + Develop priorities and classification of business processes and functions.
  + Develop recovery time requirements.
  + Determine financial, operational, and legal impacts of disruption.

The results of the BIA will impact how the DR plan develops. In particular, there are two specific BIA metrics that will impact the disaster recovery plan.

* **Recovery Point Objective (RPO**): The amount of data that a mission/business process data can afford to lose (taking into account the most recent backup of the data) following a disruption or system outage.
  + For example, if your company performs weekly backups, they have determined that they can tolerate and recover from a week’s loss of data.
* **Maximum Tolerable Downtime (MTD)**: The total amount of downtime that a system can be unavailable to users and the business. Within the time span of MTD, there are two other metrics:
  + **Recovery Time Objective (RTO)**: The maximum tolerable amount of time needed to bring all critical systems back online after a disaster.
  + **Work Recovery Time (WRT)**: The remaining time from the MTD after RTO. For example, if the MTD is four days and the RTO is one day, the WRT needed to get everything up and running again is three days.
    - The longer the MTD, the more costly it is to the business.
    - Shorter RTOs mean more costs will need to be allotted to recovery efforts.

Disaster recovery plans will vary by organization. Recovery priorities are dependent on the above metrics as well as outage impacts, resource availability, and costs.

One last major consideration for disaster recovery is having alternate sites to house critical data and technology functions. While rare, disasters may require operations be moved to an alternate site. The facility will need to support the operations established in the contingency plan.

* There are three common types of alternate sites: hot sites, cold sites, and warm sites.
  + A hot site is one that is ready to go and running at all time, and and can immediately continue operations. It will have equipment set up with current available data. While costly, hot sites are important to have for mission-critical data.
  + A cold site is a space with very little setup. These are typically not set up until a disaster occurs, and there should be a strategy in place for rapid setup. While the costs of maintaining a cold site are less expensive, these are not ideal for mission-critical data.
  + A warm site is in between. For example, servers, hardware, software, and other equipment might be set up but not be loaded with the latest data. There should be a plan for getting this data in place.
* Comprehensive business continuity planning and disaster recovery is outside of the scope of this course.