**The data lifecycle**

Organizations of all sizes handle a large amount of data that must be kept private. You learned that data can be vulnerable whether it is at rest, in use, or in transit. Regardless of the state it is in, information should be kept private by limiting access and authorization.

In security, data vulnerabilities are often mapped in a model known as the data lifecycle. Each stage of the data lifecycle plays an important role in the security controls that are put in place to maintain the CIA triad of information. In this reading, you will learn about the data lifecycle, the plans that determine how data is protected, and the specific types of data that require extra attention.

**The data lifecycle**

The data lifecycle is an important model that security teams consider when protecting information. It influences how they set policies that align with business objectives. It also plays an important role in the technologies security teams use to make information accessible.

In general, the data lifecycle has five stages. Each describe how data flows through an organization from the moment it is created until it is no longer useful:

* Collect
* Store
* Use
* Archive
* Destroy

A diagram of data lifecycle

AI-generated content may be incorrect.

Protecting information at each stage of this process describes the need to keep it accessible and recoverable should something go wrong.

**Data governance**

Businesses handle massive amounts of data every day. New information is constantly being collected from internal and external sources. A structured approach to managing all of this data is the best way to keep it private and secure.

*Data governance* is a set of processes that define how an organization manages information. Governance often includes policies that specify how to keep data private, accurate, available, and secure throughout its lifecycle.

Effective data governance is a collaborative activity that relies on people. Data governance policies commonly categorize individuals into a specific role:

* **Data owner:** the person that decides who can access, edit, use, or destroy their information.
* **Data custodian**: anyone or anything that's responsible for the safe handling, transport, and storage of information.
* **Data steward**: the person or group that maintains and implements data governance policies set by an organization.

Businesses store, move, and transform data using a wide range of IT systems. Data governance policies often assign accountability to data owners, custodians, and stewards.

**Note:** As a data custodian, you will primarily be  responsible for maintaining security and privacy rules for your organization.

**Protecting data at every stage**

Most security plans include a specific policy that outlines how information will be managed across an organization. This is known as a data governance policy. These documents clearly define procedures that should be followed to participate in keeping data safe. They place limits on who or what can access data. Security professionals are important participants in data governance. As a data custodian, you will be responsible for ensuring that data isn’t damaged, stolen, or misused.

**Legally protected information**

Data is more than just a bunch of 1s and 0s being processed by a computer. Data can represent someone's personal thoughts, actions, and choices. It can represent a purchase, a sensitive medical decision, and everything in between. For this reason, data owners should be the ones deciding whether or not to share their data. As a security professional, protecting a person's data privacy decisions must always be respected.

Securing data can be challenging. In large part, that's because data owners generate more data than they can manage. As a result, data custodians and stewards sometimes lack direct, explicit instructions on how they should handle specific types of data. Governments and other regulatory agencies have bridged this gap by creating rules that specify the types of information that organizations must protect by default:

* **PII** is any information used to infer an individual's identity. Personally identifiable information, or PII, refers to information that can be used to contact or locate someone.
* **PHI** stands for protected health information.  In the U.S., it is regulated by the Health Insurance Portability and Accountability Act (HIPAA), which defines PHI as “information that relates to the past, present, or future physical or mental health or condition of an individual.” In the EU, PHI has a similar definition but it is regulated by the General Data Protection Regulation (GDPR).
* **SPII** is a specific type of PII that falls under stricter handling guidelines. The *S* stands for sensitive, meaning this is a type of personally identifiable information that should only be accessed on a need-to-know basis, such as a bank account number or login credentials.

Overall, it's important to protect all types of personal information from unauthorized use and disclosure.

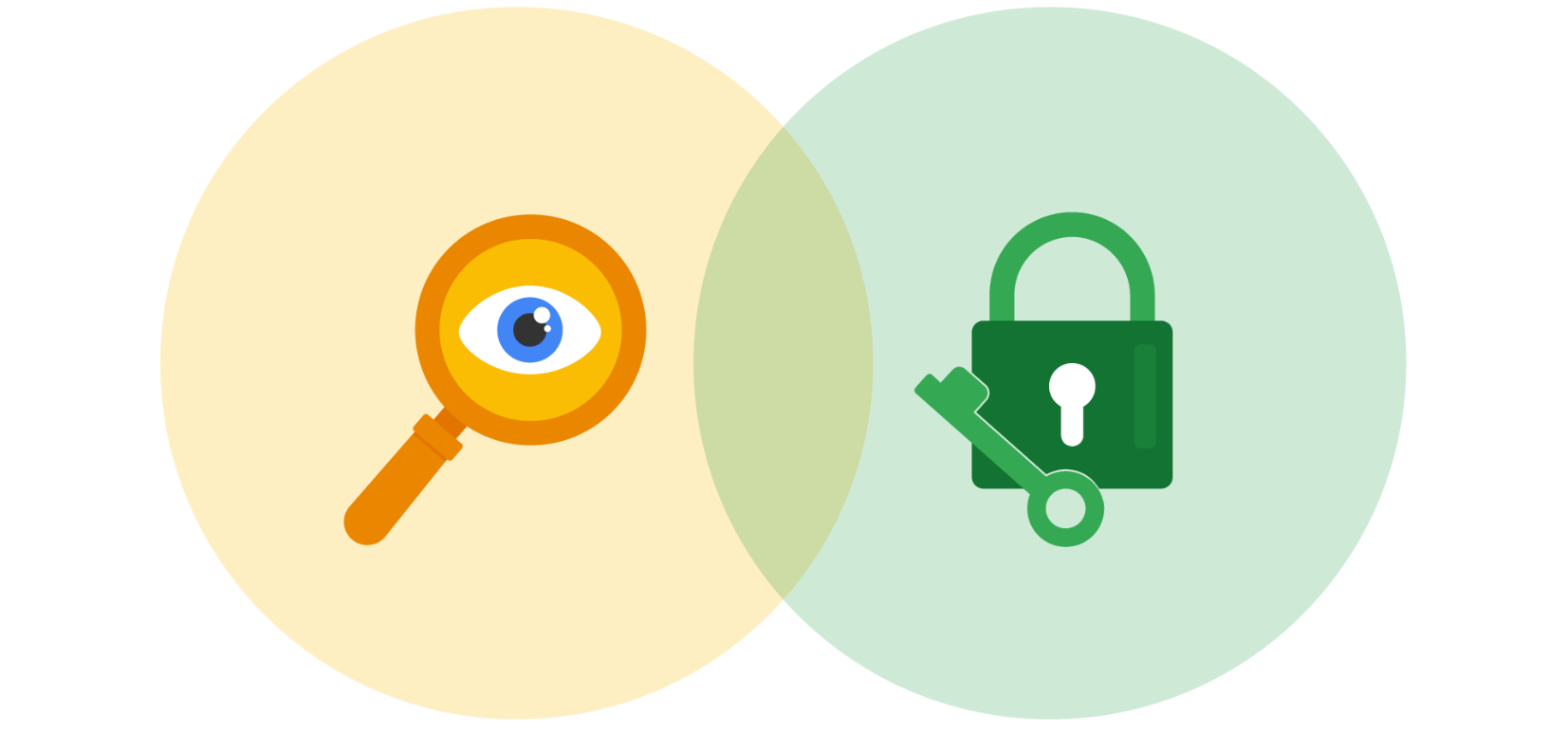
**Key takeaways**

Keeping information private has never been so important. Many organizations have data governance policies that outline how they plan to protect sensitive information. As a data custodian, you will play a key role in keeping information accessible and safe throughout its lifecycle. There are various types of information and controls that you’ll encounter in the field. As you continue through this course, you’ll learn more about major security controls that keep data private.

**Information privacy: Regulations and compliance**

Security and privacy have a close relationship. As you may recall, people have the right to control how their personal data is collected and used. Organizations also have a responsibility to protect the information they are collecting from being compromised or misused. As a security professional, you will be highly involved in these efforts.

Previously, you learned how regulations and compliance reduce security risk. To review, refer to [the reading about how security controls, frameworks, and compliance regulations](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) are used together to manage security and minimize risk. In this reading, you will learn how information privacy regulations affect data handling practices. You'll also learn about some of the most influential security regulations in the world.



**Information security vs. information privacy**

Security and privacy are two terms that often get used interchangeably outside of this field. Although the two concepts are connected, they represent specific functions:

* **Information privacy** refers to the protection of unauthorized access and distribution of data.
* **Information security** (InfoSec) refers to the practice of keeping data in all states away from unauthorized users.

The key difference: Privacy is about providing people with control over their personal information and how it's shared. Security is about protecting people’s choices and keeping their information safe from potential threats.

For example, a retail company might want to collect specific kinds of personal information about its customers for marketing purposes, like their age, gender, and location. How this private information will be used should be disclosed to customers before it's collected. In addition, customers should be given an option to opt-out if they decide not to share their data.

Once the company obtains consent to collect personal information, it might implement specific security controls in place to protect that private data from unauthorized access, use, or disclosure. The company should also have security controls in place to respect the privacy of all stakeholders and anyone who chose to opt-out.

**Note:** Privacy and security are both essential for maintaining customer trust and brand reputation.

**Why privacy matters in security**

Data privacy and protection are topics that started gaining a lot of attention in the late 1990s. At that time, tech companies suddenly went from processing people’s data to storing and using it for business purposes. For example, if a user searched for a product online, companies began storing and sharing access to information about that user’s search history with other companies. Businesses were then able to deliver personalized shopping experiences to the user for free.

Eventually this practice led to a global conversation about whether these organizations had the right to collect and share someone’s private data. Additionally, the issue of data security became a greater concern; the more organizations collected data, the more vulnerable it was to being abused, misused, or stolen.

Many organizations became more concerned about the issues of data privacy. Businesses became more transparent about how they were collecting, storing, and using information. They also began implementing more security measures to protect people's data privacy. However, without clear rules in place, protections were inconsistently applied.

**Note:** The more data is collected, stored, and used, the more vulnerable it is to breaches and threats.

**Notable privacy regulations**

Businesses are required to abide by certain laws to operate. As you might recall, **regulations** are rules set by a government or another authority to control the way something is done. Privacy regulations in particular exist to protect a user from having their information collected, used, or shared without their consent. Regulations may also describe the security measures that need to be in place to keep private information away from threats.

Three of the most influential industry regulations that every security professional should know about are:

* General Data Protection Regulation (GDPR)
* Payment Card Industry Data Security Standard (PCI DSS)
* Health Insurance Portability and Accountability Act (HIPAA)

**GDPR**

GDPR is a set of rules and regulations developed by the European Union (EU) that puts data owners in total control of their personal information. Under GDPR, types of personal information include a person's name, address, phone number, financial information, and medical information.

The GDPR applies to any business that handles the data of EU citizens or residents, regardless of where that business operates. For example, a US based company that handles the data of EU visitors to their website is subject to the GDPRs provisions.

**PCI DSS**

PCI DSS is a set of security standards formed by major organizations in the financial industry. This regulation aims to secure credit and debit card transactions against data theft and fraud.

**HIPAA**

HIPAA is a U.S. law that requires the protection of sensitive patient health information. HIPAA prohibits the disclosure of a person's medical information without their knowledge and consent.

**Note:** These regulations influence data handling at many organizations around the world even though they were developed by specific nations.

Several other security and privacy compliance laws exist. Which ones your organization needs to follow will depend on the industry and the area of authority. Regardless of the circumstances, regulatory compliance is important to every business.

**Security assessments and audits**

Businesses should comply with important regulations in their industry. Doing so validates that they have met a minimum level of security while also demonstrating their dedication to maintaining data privacy.

Meeting compliance standards is usually a continual, two-part process of security audits and assessments:

* A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations.
* A **security assessment** is a check to determine how resilient current security implementations are against threats.

For example, if a regulation states that multi-factor authentication (MFA) must be enabled for all administrator accounts, an audit might be conducted to check those user accounts for compliance. After the audit, the internal team might perform a security assessment that determines many users are using weak passwords. Based on their assessment, the team could decide to enable MFA on all user accounts to improve their overall security posture.

**Note:** Compliance with legal regulations, such as GDPR, can be determined during audits.

As a security analyst, you are likely to be involved with security audits and assessments in the field. Businesses usually perform security audits less frequently, approximately once per year. Security audits may be performed both internally and externally by different third-party groups.

In contrast, security assessments are usually performed more frequently, about every three-to-six months. Security assessments are typically performed by internal employees, often as preparation for a security audit. Both evaluations are incredibly important ways to ensure that your systems are effectively protecting everyone's privacy.

**Key takeaways**

A growing number of businesses are making it a priority to protect and govern the use of sensitive data to maintain customer trust. Security professionals should think about data and the need for privacy in these terms. Organizations commonly use security assessments and audits to evaluate gaps in their security plans. While it is possible to overlook or delay addressing the results of an assessment, doing so can have serious business consequences, such as fines or data breaches.

**Protecting Personally Identifiable Information (PII)**

**PII** (Personally Identifiable Information) is everywhere in our digital lives. It includes both **public** and **sensitive** data:

* **Public PII**: Name, general contact information.
* **Sensitive PII**: Bank details, medical records, Social Security numbers.

Since we conduct activities like **banking, voting, and registrations** online, **built-in security** is crucial.

**Best Practices for PII Protection**

1. **Encrypt Data**
   * **At rest**: Encrypt stored data to prevent unauthorized access.
   * **In transit**: Use **TLS (Transport Layer Security) or SSL (Secure Sockets Layer)** to protect data moving across networks.
2. **Restrict Access**
   * **Limit data access** to only those who truly need it.
   * **Keep records** of who accessed sensitive data and why.
   * **Review audit logs** regularly for unauthorized access.
3. **Respond Thoughtfully to Breaches**
   * **Understand the impact**: PII compromise affects real people.
   * **Be transparent**: Users must **trust** the systems and infrastructure.
   * **Take action**: Investigate breaches, notify affected users, and strengthen security.

**Final Thought**

**Trust is the foundation** of online security. Organizations must **proactively protect** PII to ensure users feel safe and confident in the digital world.