aws re/start

Introduction to Security

What you will learn

At the core of the lesson

You will learn how to:

- Define security in terms of the confidentiality, integrity, and availability (CIA) triad
- Identify different types of threats
- Identify the components that comprise a security strategy
- Explain the difference between hacking, cracking, and penetration testing
- Name the stages of the security lifecycle
- Describe how cyber laws and regulations impact organizational security policy

What is security?

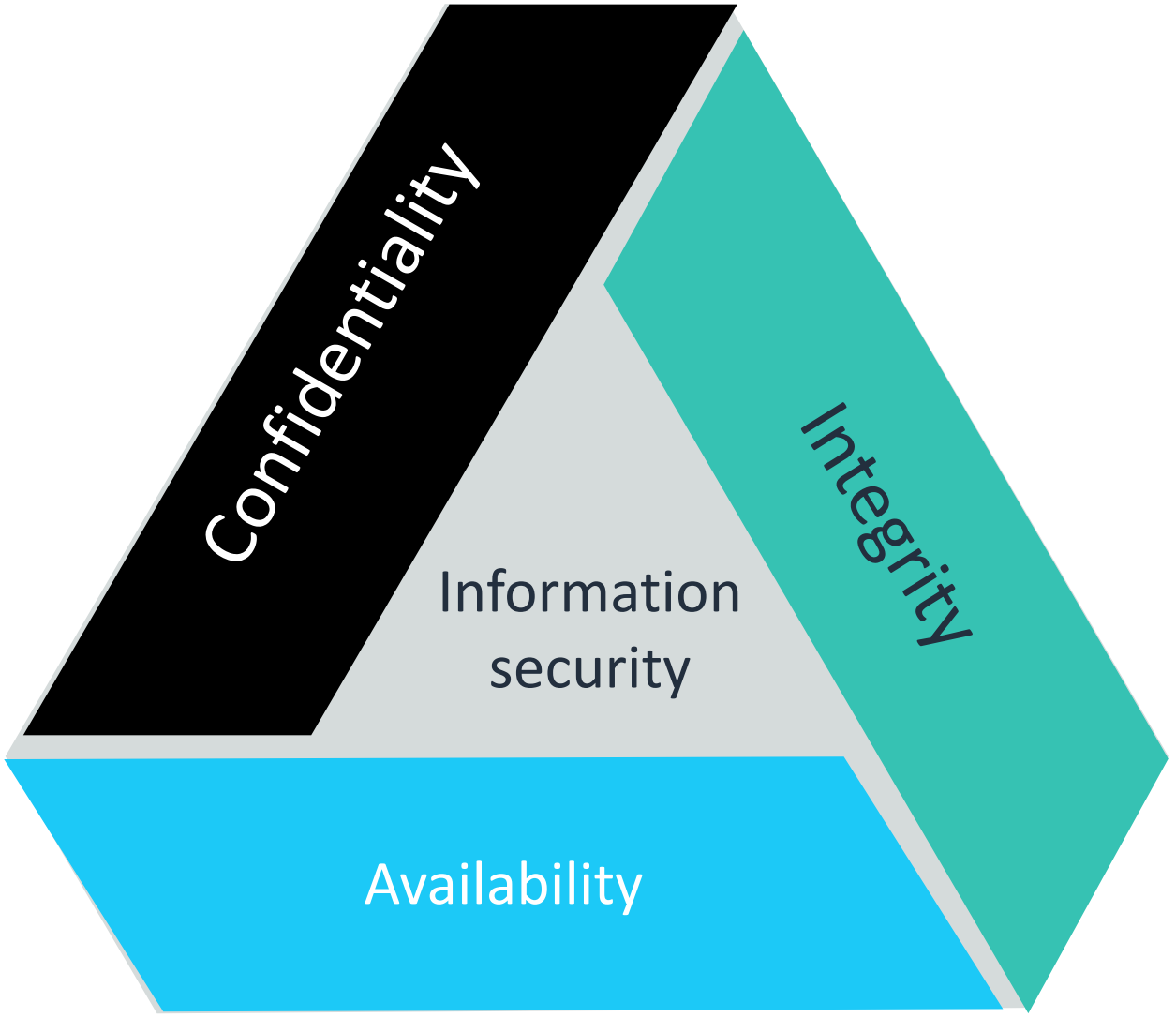
Discussion: Security introduction

What would be the impact on your life if the internet was down for a few days?

What would be the impact if your personal information was stolen?

What kinds of controls do you have in place to prevent any of this from happening?

What is security?



Why is security important?

Poor security leaves personnel and organizations open to the following security risks:

Identity theft

Data theft

Loss of network services and resources

Loss of or damaged business reputation

Corporate sabotage or espionage

Types of threats

- Appropriate security helps mitigate the following types of threats:
  - Malware
  - Password events (dictionary, brute force)
  - Distributed denial of service (DDoS)
  - Man-in-the-middle (MitM)
  - Phishing
  - Social engineering
  - Drive-by

Security strategy

Types of security

System security

Infrastructure security

Access management

Identity management

Data security

Software security

Physical security

Strategy

Physical security

Access management

Known security risks and common exploits

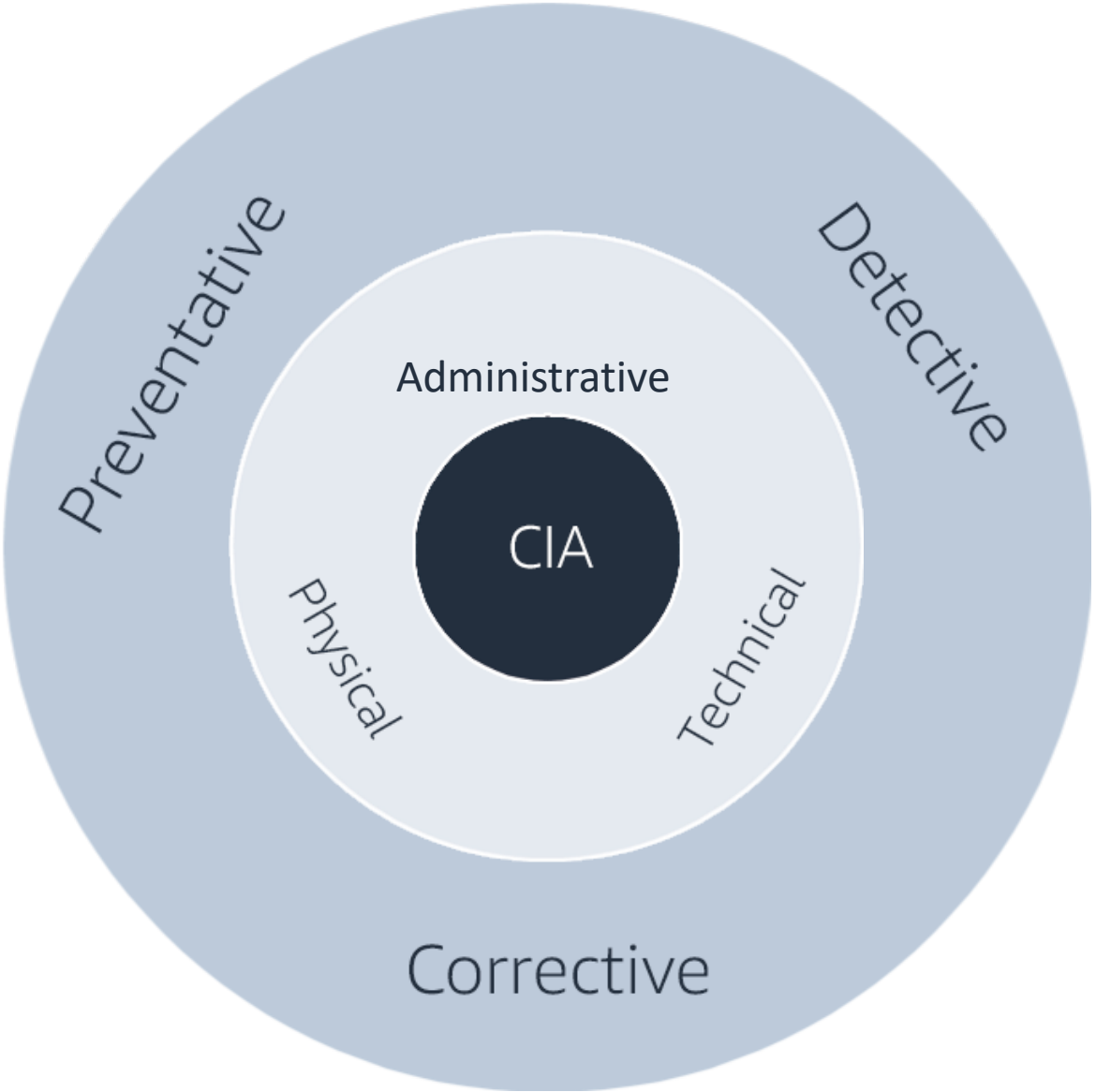
Policies and procedures

Discussion

Companies can implement different levels and types of security controls.

What are the drivers for the security controls that are implemented in modern networks and organizations?

Security controls

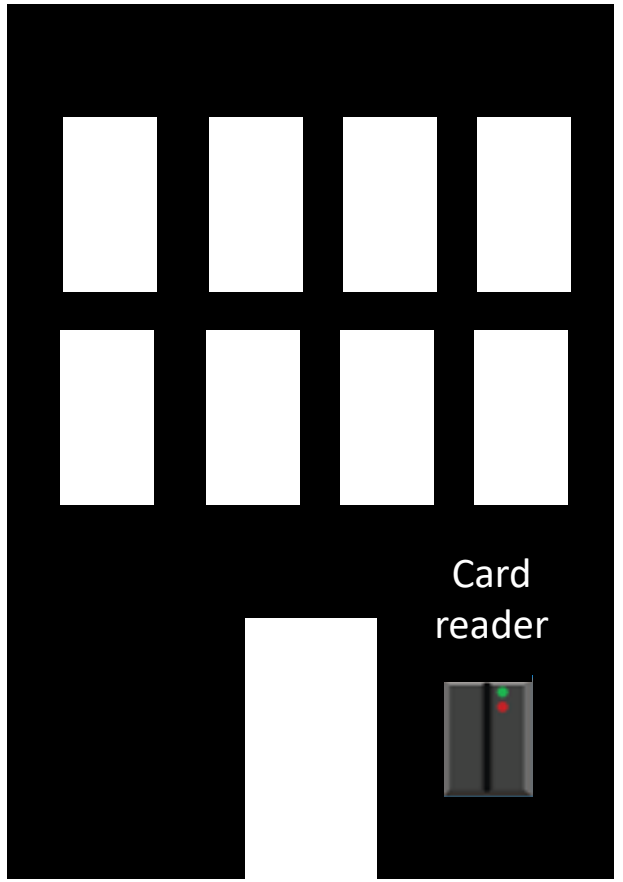


Compensating security controls

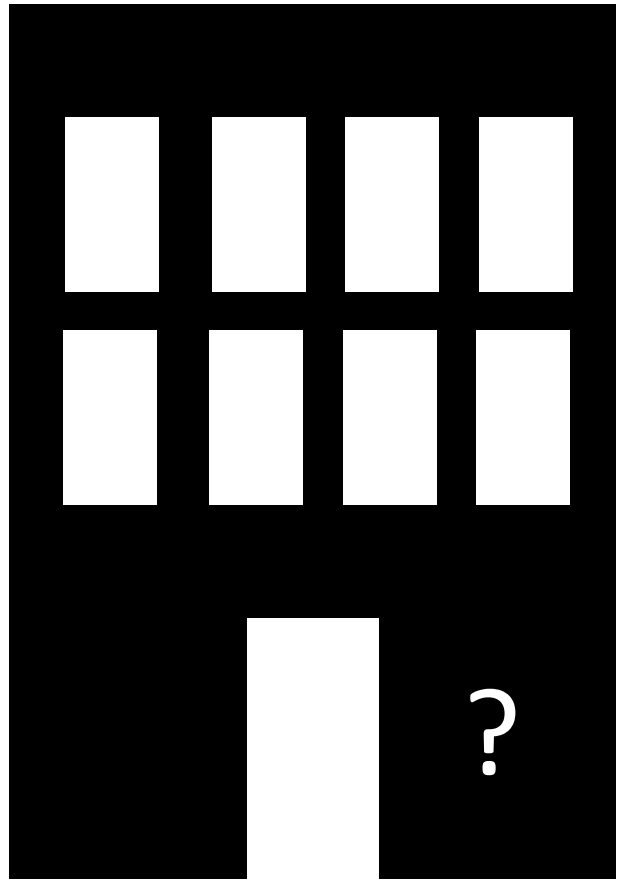
Your main data center has a card reader system. When you go to an alternate site, the data center doesn't have that same system.

What do you do to control who can enter the alternate data center?

Primary data center



Alternate data center



What is hacking?

Risk vectors and targets can be:

- Physical
- Technical
- Social

Hacking and cracking

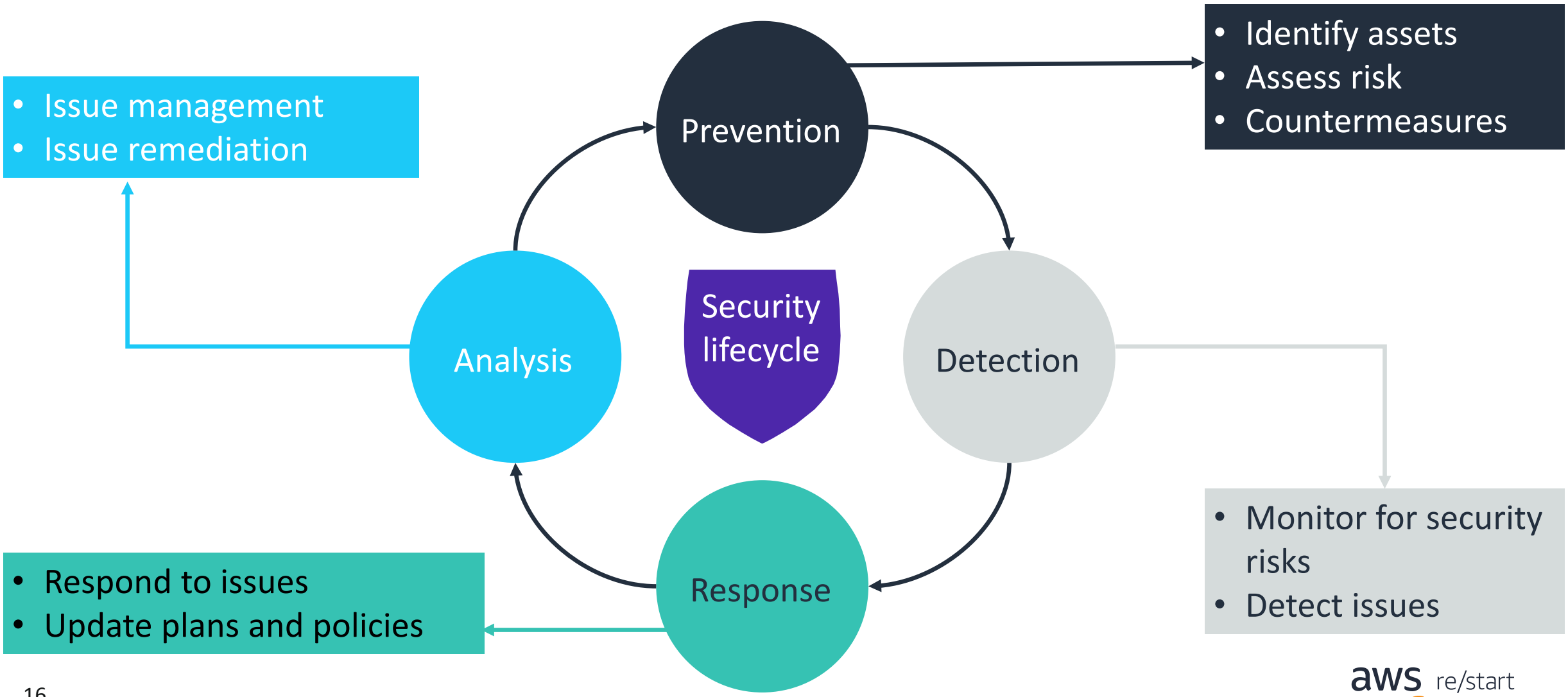
Unauthorized access

Penetration testing

Tests for potential compromises

Security lifecycle

Security lifecycle



Discussion

What does the security lifecycle look like in a real-world situation?

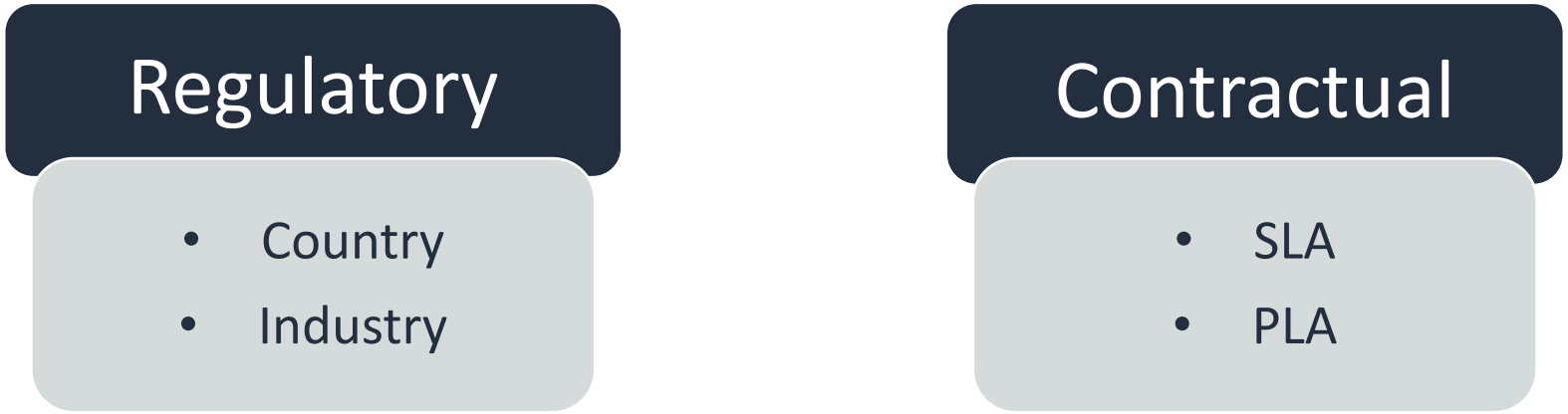
How does the security lifecycle differ between industries?

Who sets the rules for individual security need?

Regulatory compliance

Regulatory compliance

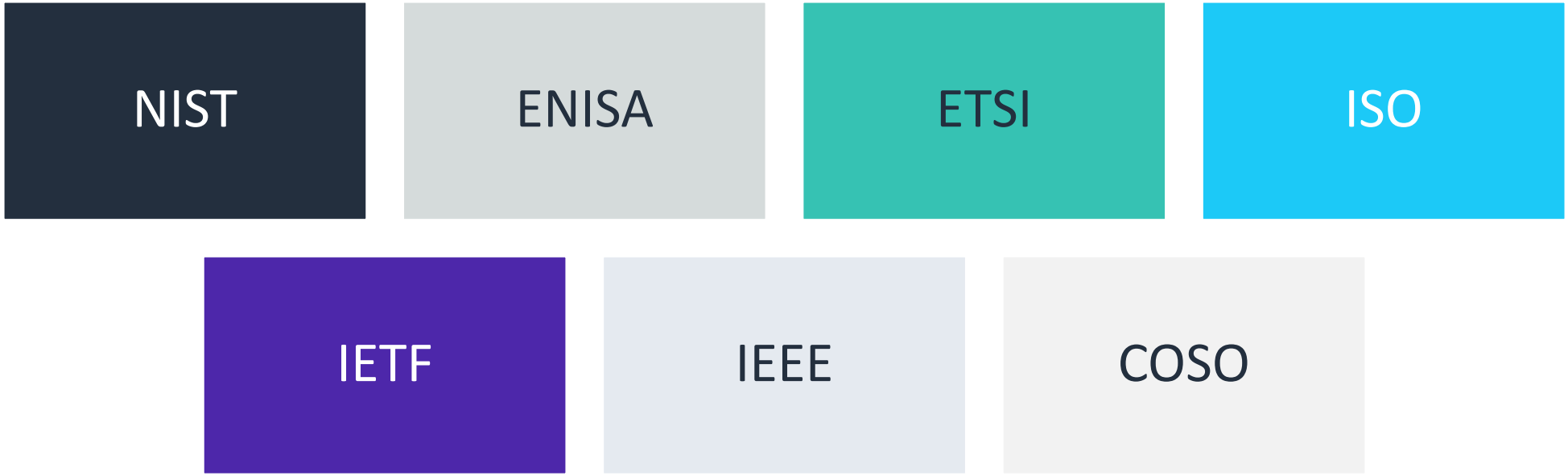
- Security controls are often mandated by regulations.



- Avoid conflicts among different localities, jurisdictions, or cultures.

Cybersecurity standards

- Standards in IT continue to evolve. No single standard is foolproof or future-proof for your environment.
- Organizations focused on developing standards:



Compliance

- External authority:
  - *Government or laws*. Mandatory compliance
  - *Open standards*. Compliance required to participate
  - *Best practices*. Optional compliance
- Non-compliance has consequences:
  - *Government or laws*. Civil, criminal, or financial penalties
  - *Open standards*. Financial penalties or participation is denied
  - *Best practices*. Loss of customers, partners, or revenue
- Proper reporting is required to prove compliance.

Payment card industry (PCI) security standard

- PCI is a regulated set of requirements intended to maintain a secure environment.
  - Requirements focus on various aspects of data security.
- All entities involved in processing payment card data must comply with PCI Security Standards.
- PCI Security Standards Council also provides security assessment procedures.

Compliance standards: European Union

At its core, **General Data Protection Regulation (GDPR)** is a set of regulations created to provide ***European Union (EU)*** **citizens** more enhanced control over their data.

United States: HIPAA

- U.S. Health Insurance Portability and Accountability Act of 1996
  - Modernized the handling of healthcare information.
  - Stipulates how personally identifiable information should be protected.
  - Addresses limitations on healthcare insurance coverage.
  - Consists of five titles that specify the laws of the act.

- Example: Healthcare providers do not disclose identities of patients over the phone to family members.

Compliance standards: European Union

At its core, **General Data Protection Regulation (GDPR)** is a set of regulations created to provide ***European Union (EU)*** **citizens** more enhanced control over their data.

Compliance standards: Russia

Russian federal law on personal data:

- Consent of the individual is required.
- A personal data subject can revoke their previously granted consent.
- The transfer of personal data outside the Russian federation requires adequate protection in the destination country.

Compliance standards: China

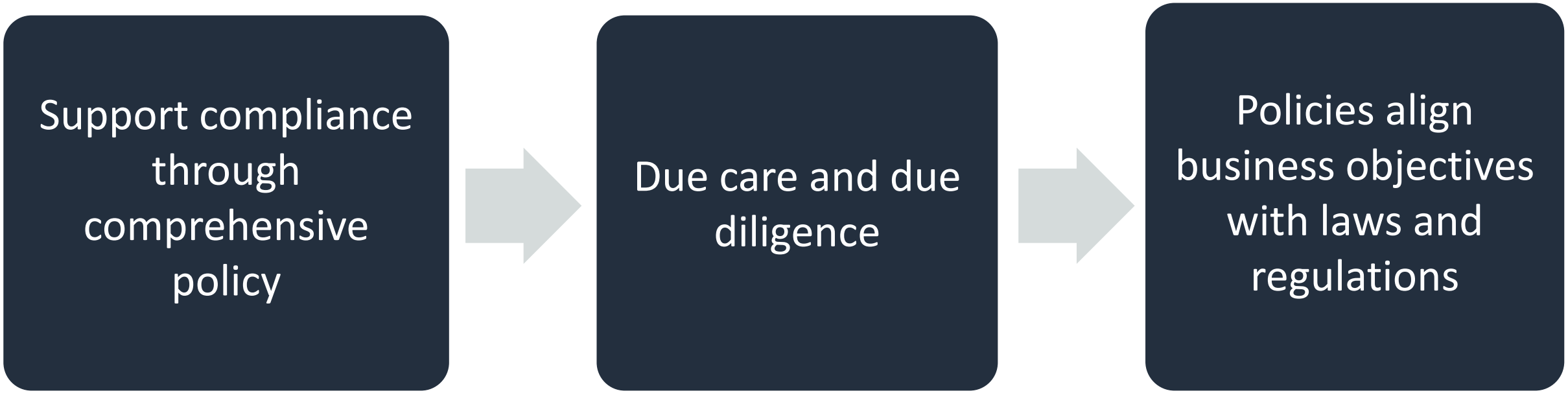
Cybersecurity law of the People's Republic of China:

- Requires select data to be stored in China.
- Allows Chinese authorities to conduct spot checks on a company’s network operations.

Other standards

Laws and Regulations	US	Canada	EU
Sarbanes-Oxley Act (SOX)	X		
Gramm-Leach-Bliley Act (GLBA)	X		
Federal Information Security Management Act (FISMA)	X		
General Data Protection Regulation (GDPR)			X
Personal Information Protection and Electronic Documents Act (PIPEDA)		X	
Financial Industry Regulatory Authority (FINRA)	X		
Family Educational Rights and Privacy Act (FERPA)	X		
Dodd-Frank Wall Street Reform and Consumer Protection Act – U.S.	X		

Compliance and company policy



Key takeaways

- Consider these perspectives when addressing information security: confidentiality, integrity, and availability.
- Common types of security issues include malware, phishing, and social engineering.
- A good security strategy implements the phases of the security lifecycle: prevention, detection, response, and analysis.
- Various industry security compliance standards exist to provide a framework for enforcing good security practices.