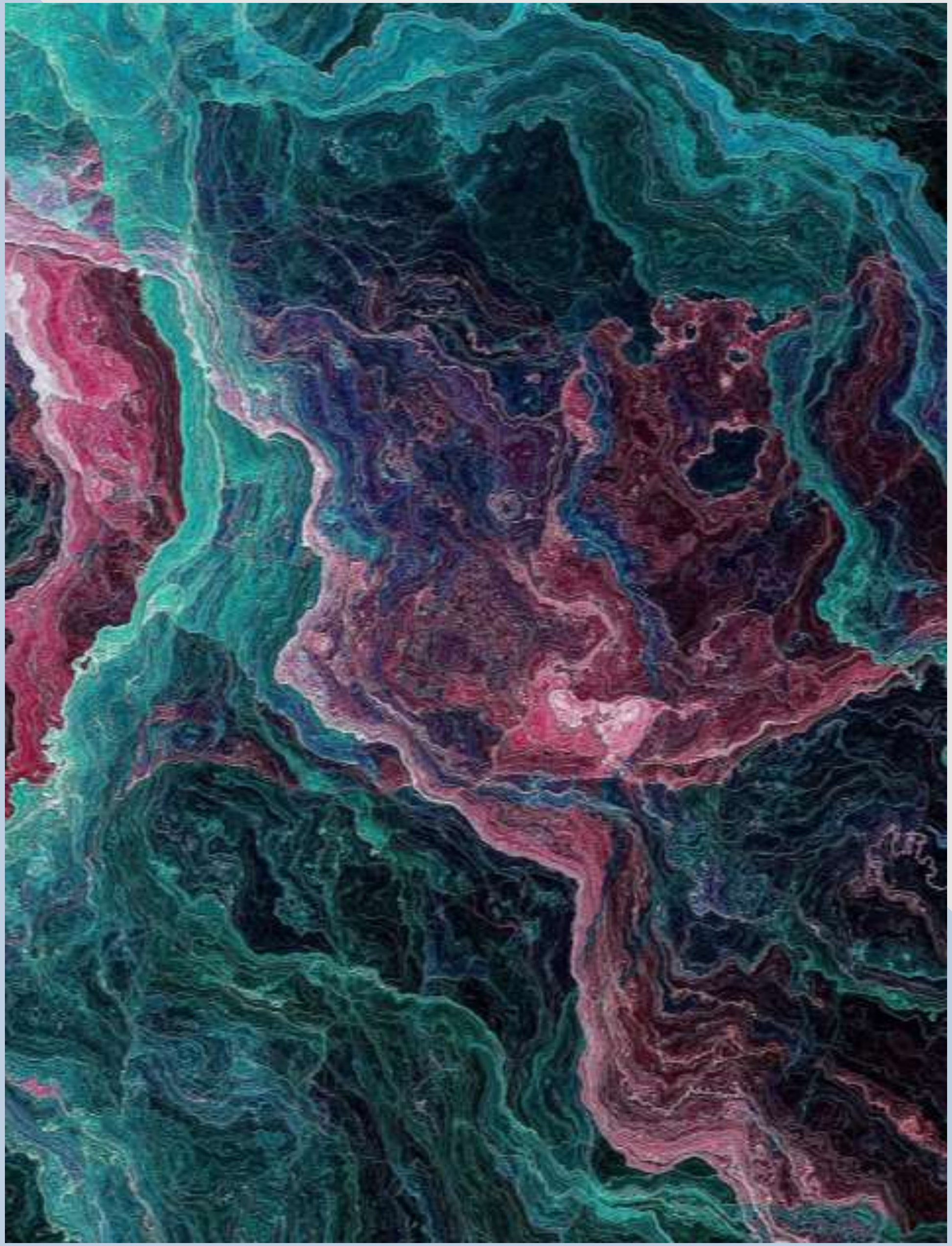


Information Security: A Strategic Risk

Lisa Thiergartner | October 6, 2022

Who Am I

Information Security - GRC

Governance

The collection of practices related to supporting, evaluating, defining, and directing the security efforts of an organization.

Risk

Evaluating the organization’s threats and vulnerabilities.

Compliance

Processes, policies, and procedures that support requirements, and guidelines established by lawmakers

PCI DSS, HIPAA Security Rule, FFIEC

Mission and Purpose

To improve an organization’s information security program using the NIST Cybersecurity framework

To build meaningful business relationships

To have fun

(R3) – Ready, Reliable and Resilient

Ready

when something happens

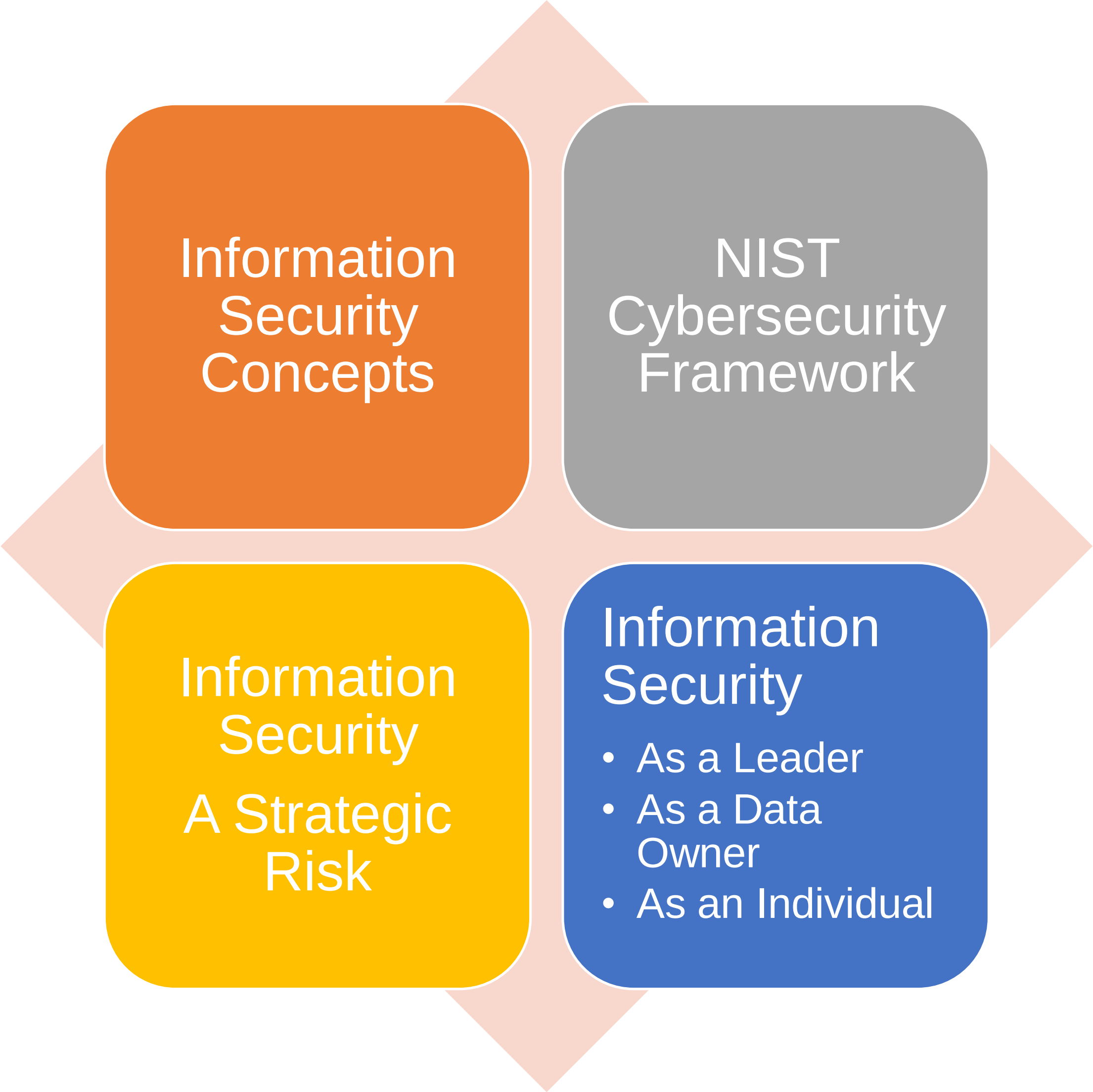
Reliable

during the situation

Resilient

after it happens

Agenda



Information Security Concepts

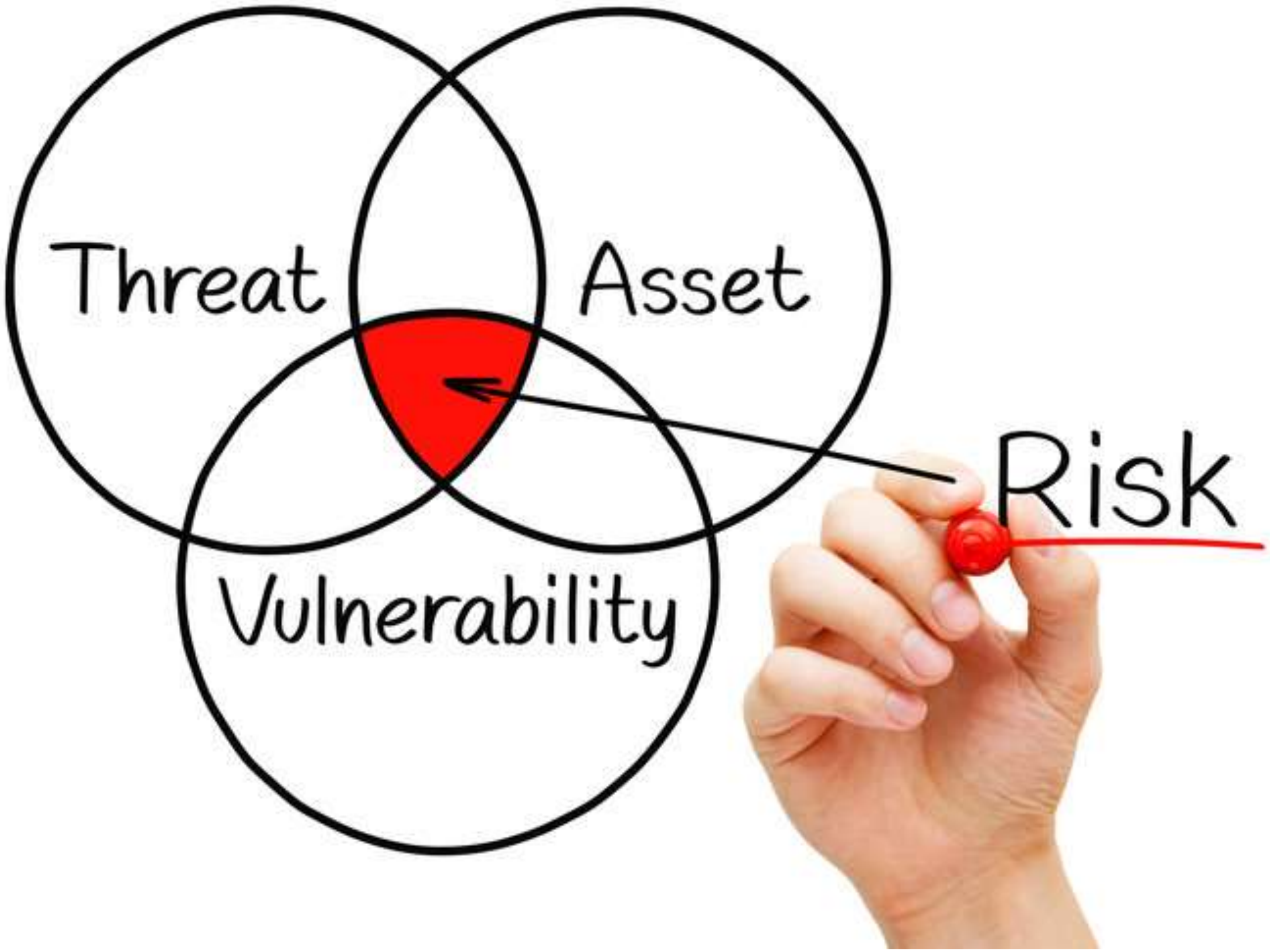
NIST Cybersecurity Framework

Information Security

A Strategic Risk

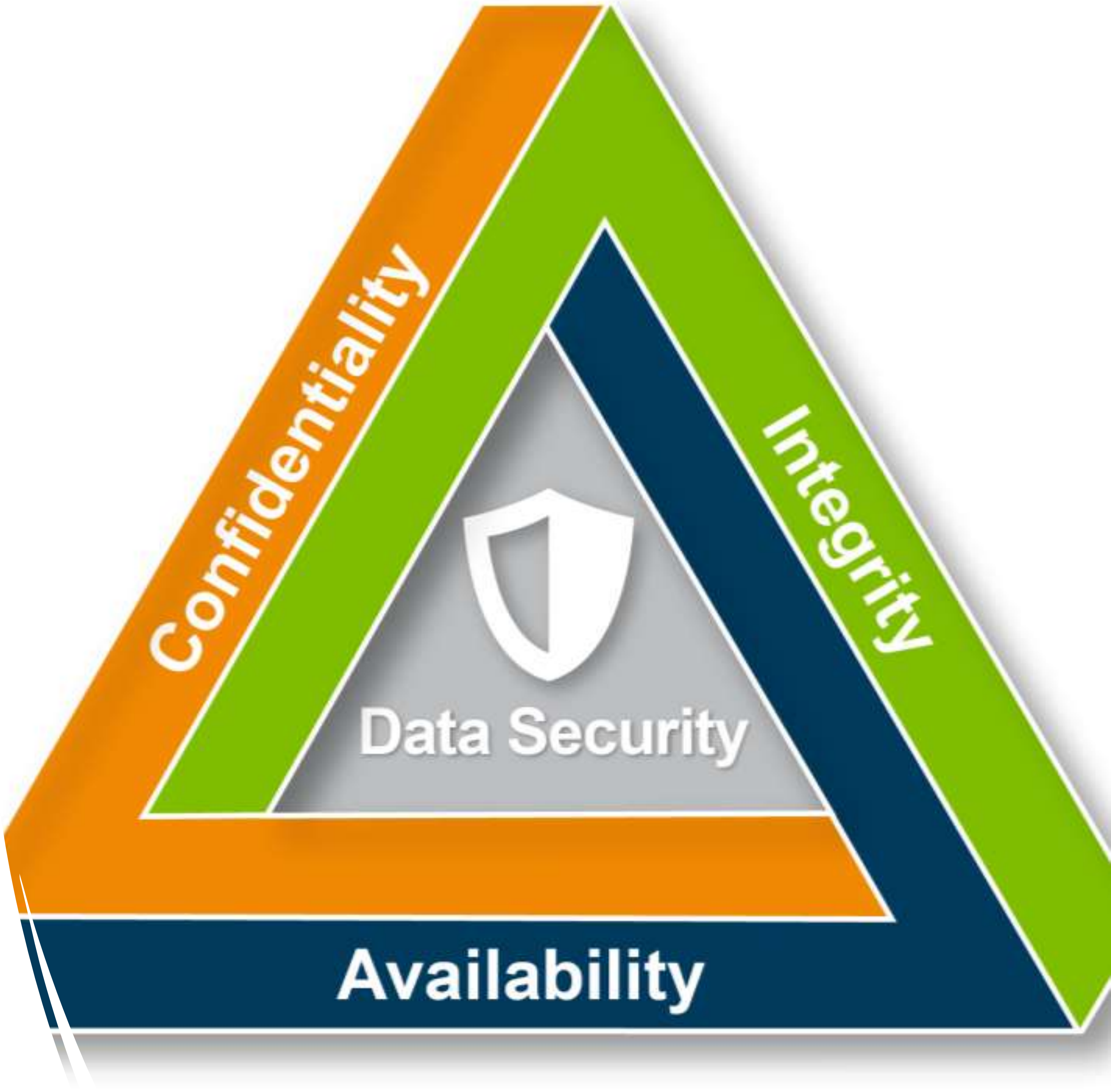
Information Security

- As a Leader
- As a Data Owner
- As an Individual


Threat
Asset
Vulnerability
Risk

CIA Triangle

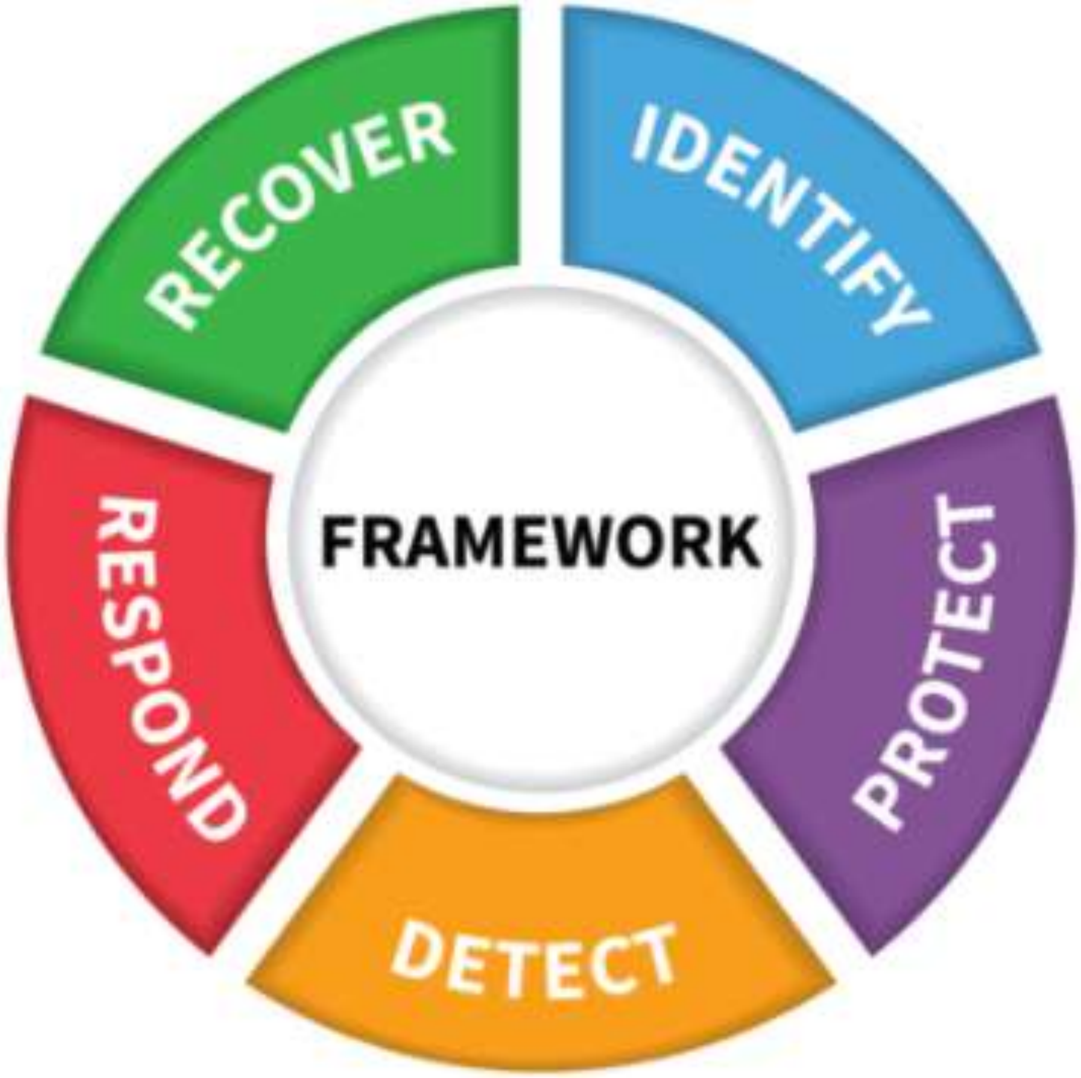
- Confidentiality
- Integrity
- Availability



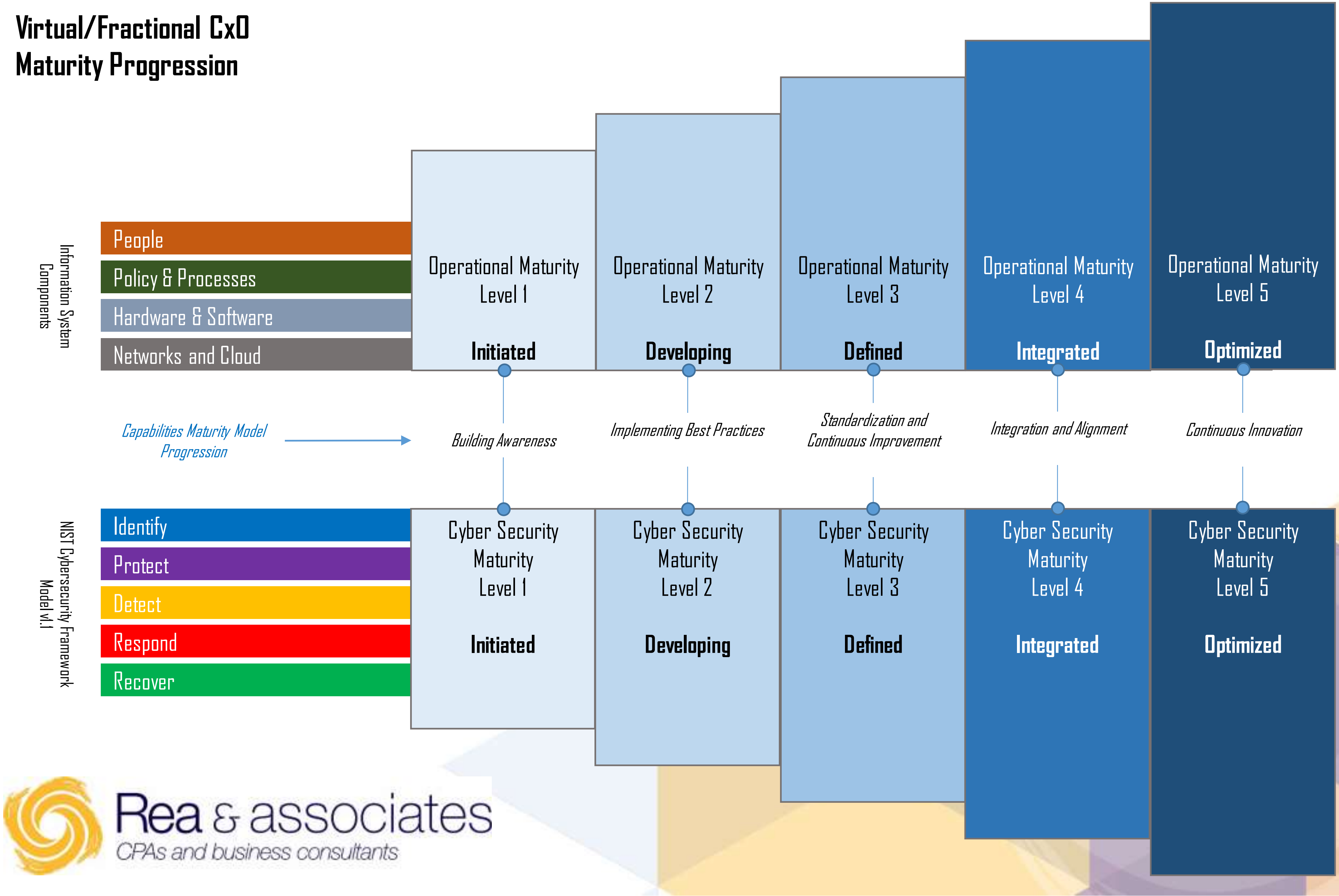
NIST Framework Attributes

Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



Virtual/Fractional CxO
Maturity Progression



Information System Components

- People
- Policy & Processes
- Hardware & Software
- Networks and Cloud

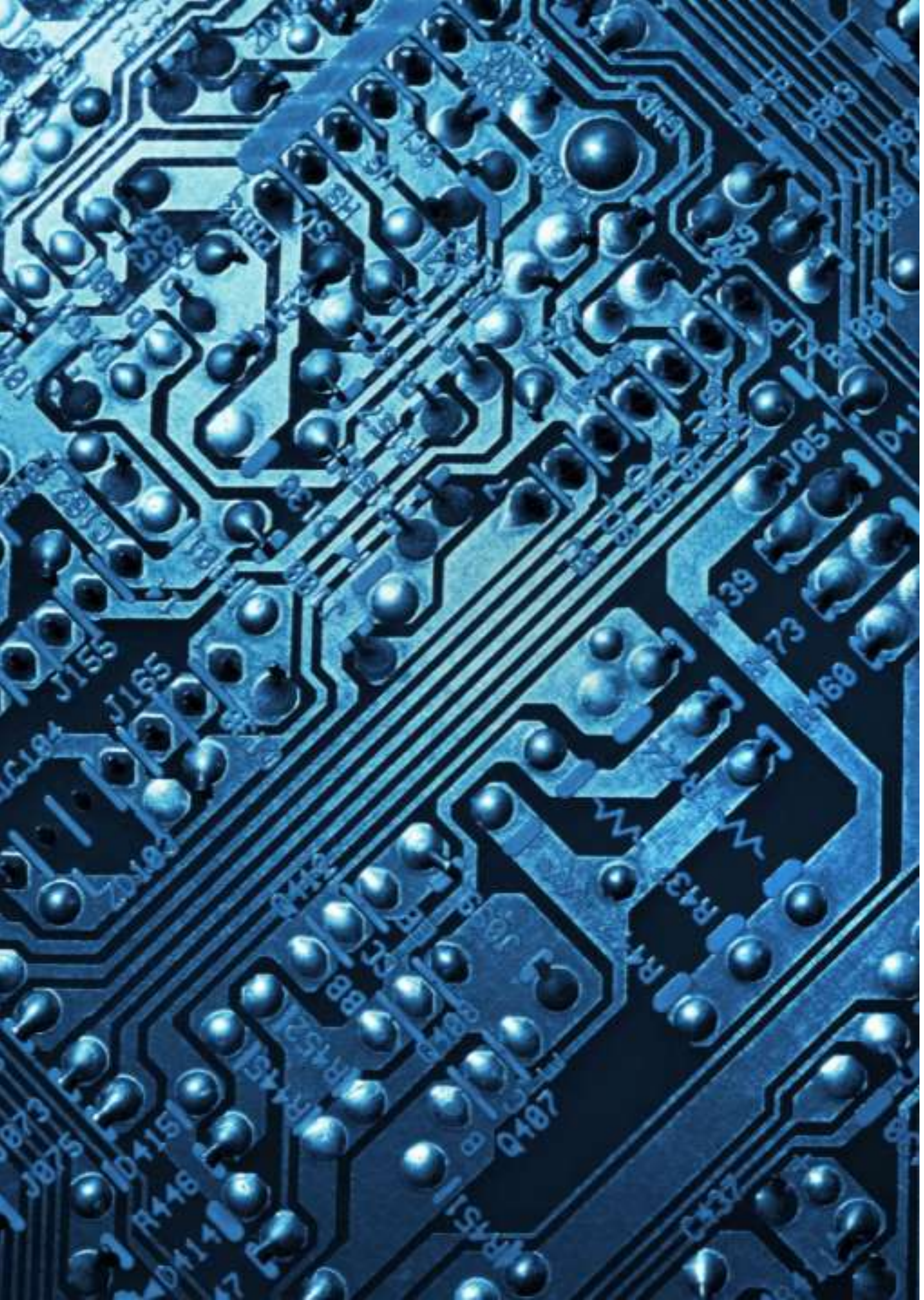
Capabilities Maturity Model Progression →

NIST Cybersecurity Framework Model v1.1

- Identify
- Protect
- Detect
- Respond
- Recover

Operational Maturity Level 1	Operational Maturity Level 2	Operational Maturity Level 3	Operational Maturity Level 4	Operational Maturity Level 5
Initiated	**Developing**	**Defined**	**Integrated**	**Optimized**
Building Awareness	*Implementing Best Practices*	*Standardization and Continuous Improvement*	*Integration and Alignment*	*Continuous Innovation*
Cyber Security Maturity Level 1	Cyber Security Maturity Level 2	Cyber Security Maturity Level 3	Cyber Security Maturity Level 4	Cyber Security Maturity Level 5
Initiated	**Developing**	**Defined**	**Integrated**	**Optimized**

Rea & associates
CPAs and business consultants



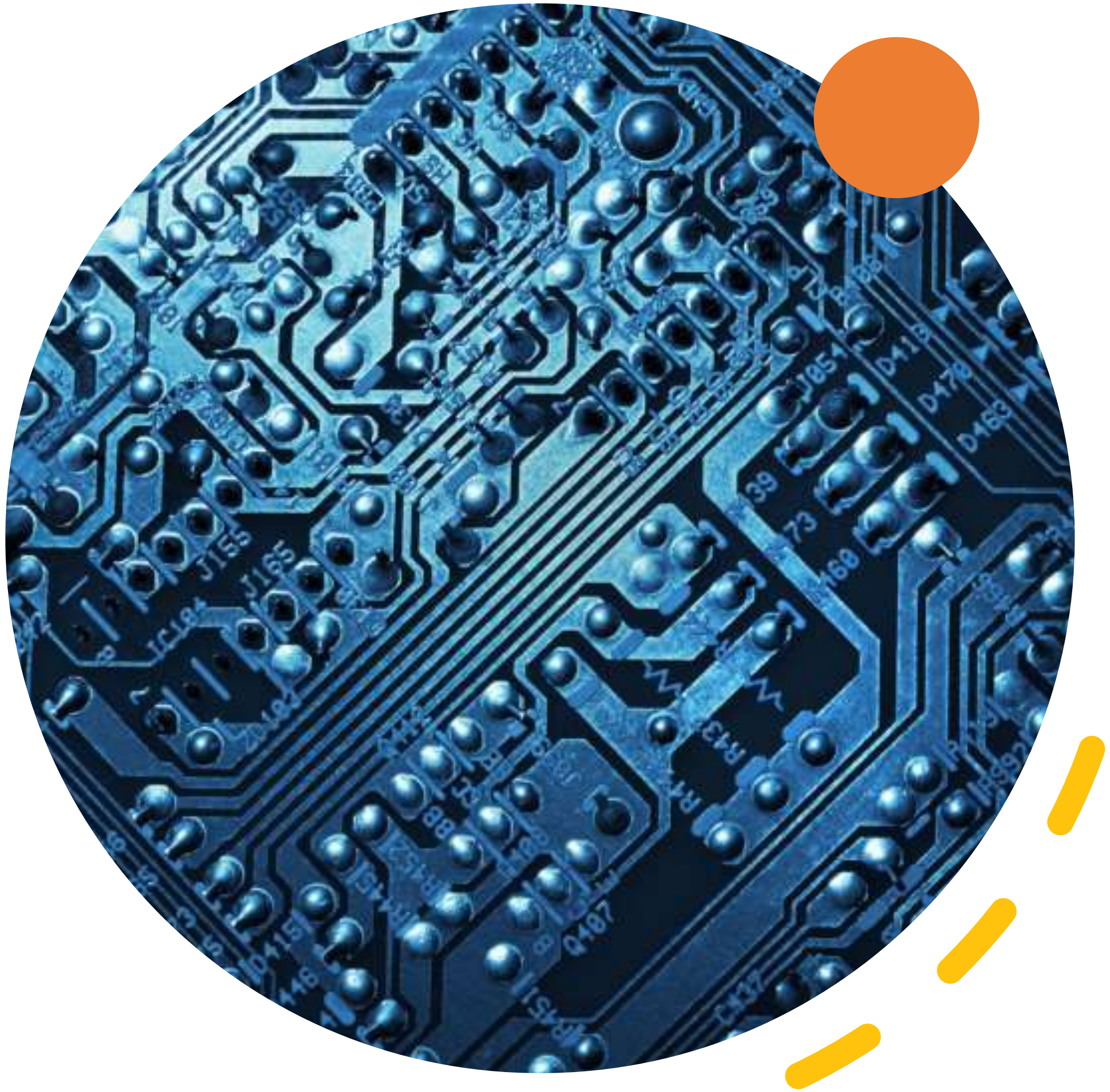
Cyber Risk Oversite

- Leaders understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.
- Leaders understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- Leaders have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
- Leaders set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.
- Leaders discuss cyber risk to include the identification and quantification of financial exposure to cyber risks.
- Determine which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

Cybersecurity
A Strategic Risk

As A Strategic Risk

- Do you have a risk-management practice to know your major risks, and understand the size of your attack surface?
- Do you assess the criticality of your digital infrastructure based on the type of business processes they support?
- Do you use inventory reviews of connected users and devices to harden systems and add resilience in a targeted and prioritized manner?
- What are the organization’s most critical data assets?
- Where do critical data assets reside? Are they located on one or multiple systems?
- How are they accessed? Who has permission to access them?
- How often are systems to make sure that they are adequately protecting our data?



Information Security
As a Leader

Cyberliteracy

- Contribute to a conversation about the current state of the company’s cybersecurity? In which areas does our lack of knowledge/understanding of cyber matters prevent effective oversight?
- Interpret/assess management’s presentations and their answers to our questions.
- Understand the most significant cyber threats to this business and what impacts they could have on the company’s strategy and ultimately on its long-term growth?
- Monitor current and potential cybersecurity-related legislation and regulation?
- Understand insurance coverage for cyber events. Is there director and officer exposure if we don’t carry adequate insurance?
- Participate in public- or private-sector ecosystem-wide cybersecurity and information-sharing organizations?

Incident Response

Incident playbook

Is there an incident playbook with clear definitions of incidents, roles and responsibilities, and escalation processes?

Escalation Criteria

What are the escalation criteria for notifying senior leadership and the board if necessary? Who has final decision-making authority?

Back Ups Tested

Is the organizational resiliency tested around large risk scenarios and exercised through tabletops and common threat simulation?

Information Sharing

Are there established relationships with the intel community and key regulators? Have information-sharing relationships been established?

Incident Disclosure

What are the criteria and what is the process for disclosing incidents?

Loss Mitigation

What can we do to mitigate the losses from an incident?

Cyber Supply-Chain Risk Management

- How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?

- What do we need to do to fully include cybersecurity in current supply-chain risk management?

- How are cybersecurity requirements built into contracts and service-level agreements? How are they enforced?

Security Culture

Every organization has a security culture.

92% of management and higher positions believe a security culture is important to the organization.

- Awareness
- Behavior
- Culture

Security Culture

Security practices are embedded into the organization.

- Humans decide what technology to purchase.
- Humans determine the need for new processes.
- Humans review third-party risk.
- Humans decide how they will respond to something that looks suspicious.
- Humans decide how they will interact with systems and information each day.

Information Security
As a Data Owner

Information Technology General Controls

- Access management and controls
- Password Policy
- Physical security of servers and user devices
- Application security and patching
- Network and endpoint security monitoring and controls
- Backup and Recovery Process
- Employee education

Privilege Access

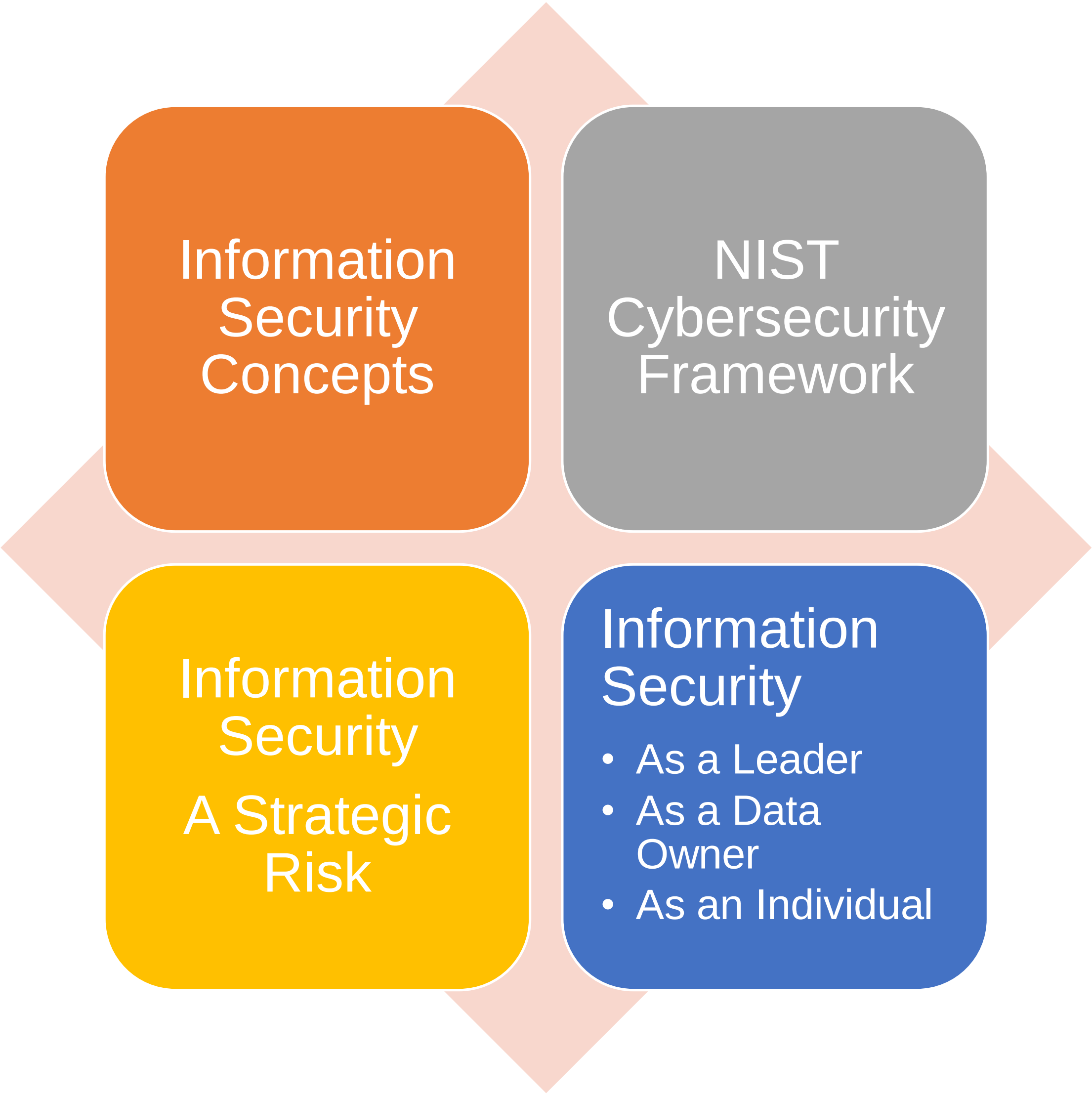
- Logging on to unsecured endpoints
- Sharing administrative accounts
- Using administrative accounts for daily activities
- Using poor password management practices
- Having too many administrative accounts in the system

Information Security As An Individual

Individual Security

- Back Up Your Data
- Enable Multi-Factor Or Two-Step Authentication
- Check The Email Address Domain
- Password Management
- Hover Over URLs Before Clicking To Ensure Legitimacy
- Read The End User License Agreement / Go to Privacy and Security Setting
- Always Use A Virtual Private Network
- Disable Location Services And Microphone Access Where Not Needed
- Don't Ignore Software And OS Updates
- Subscribe To Haveibeenpwned.com

Closing



Information Security Concepts

NIST Cybersecurity Framework

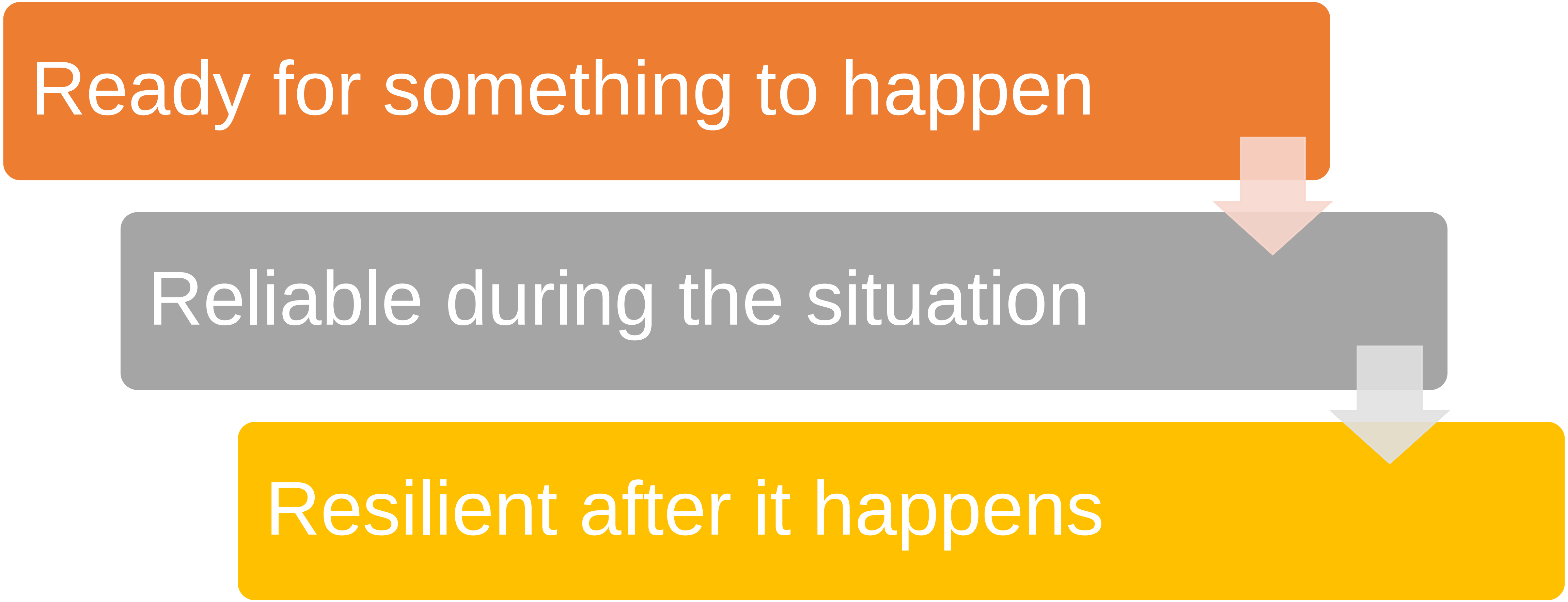
Information Security

A Strategic Risk

Information Security

- As a Leader
- As a Data Owner
- As an Individual

(R3) – Ready, Reliable and Resilient

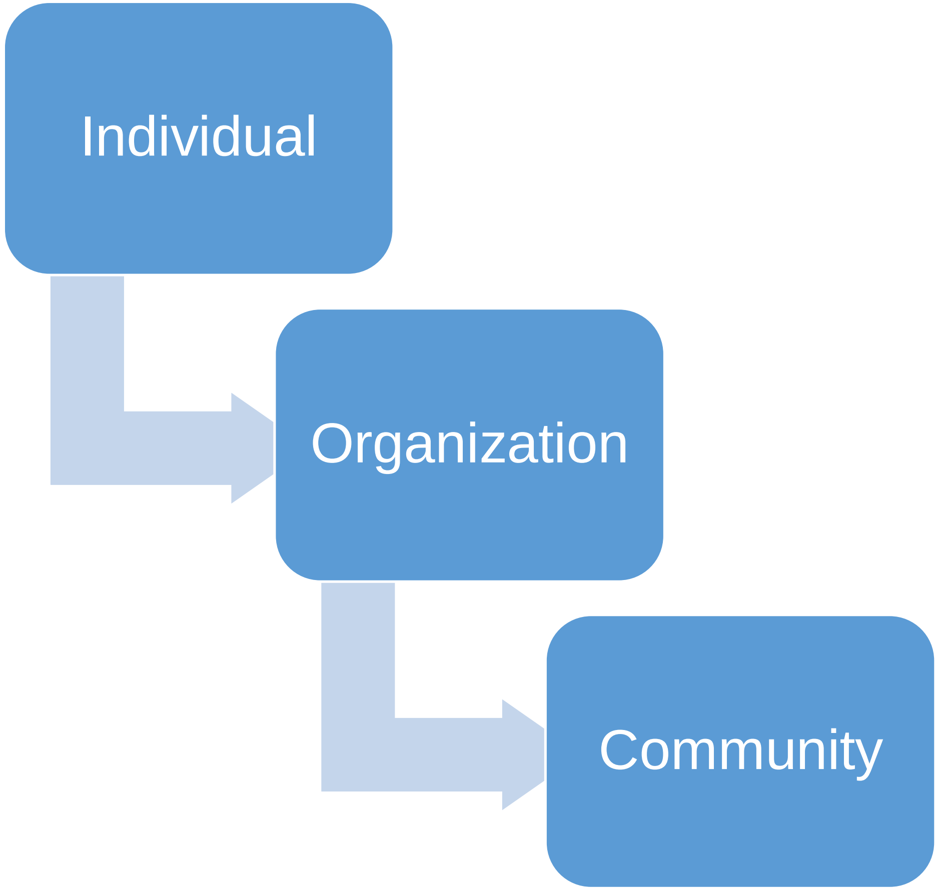


Ready for something to happen

Reliable during the situation

Resilient after it happens

Resilient



Individual

Organization

Community

Cybersecurity Awareness Month

October