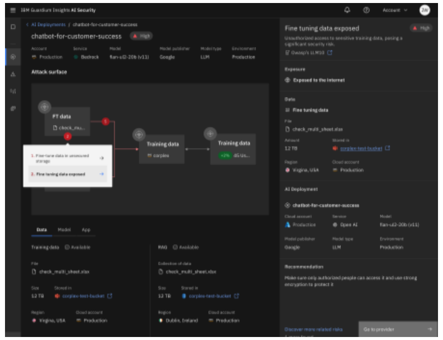
Empowering Cybersecurity Excellence

Bob Justus, IBM Security

Bob.Justus@ibm.com

New security innovation

AI Security

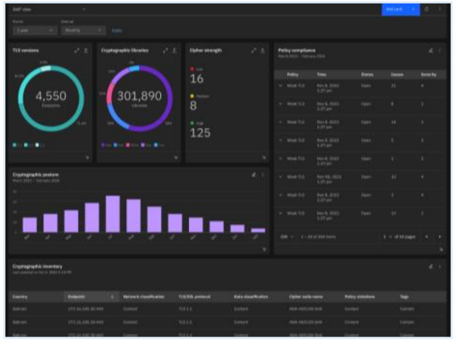


Explosive use of AI leads to unknown usage, new risks, misconfigured pipelines, vulnerable training data

New Guardium product will protect AI usage in the cloud with visibility of models, sensitive data, and risks

- Discover and protect sensitive AI training data and track its lineage
- Protect AI models from exfiltration, insider threats and 3rd party access
- Remediate AI vulnerabilities and unapproved open-source content

Quantum Safe

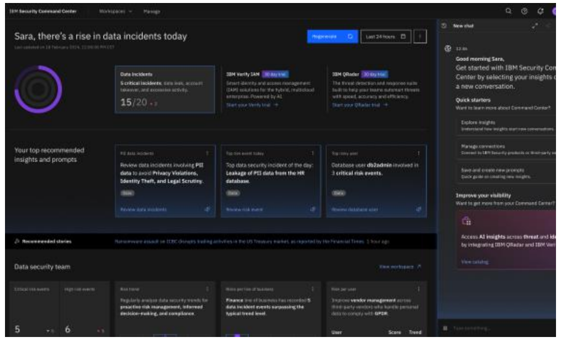


Quantum attacks will soon break encryption, exposing sensitive data that is currently protected

New Guardium product will help clients understand quantum risks, priorities, and begin remediation

- Identify at-risk crypto libraries, datastores, and applications
- Visualize and contextualize risk through dashboards and reports
- Determine remediation plans and automate suggestions

GenAI for Cybersecurity


Sara, there's a rise in data incidents today
15/20
Your top recommended insights and prompts
Data security team

Security professionals face daily repetitive, complex, and tedious tasks, while often lacking answers

New AI for cyber use cases across data, identity, and other teams to boost productivity and knowledge

- Summarize complex security events and data risk into key insights
- Generate content to stay ahead of compliance violations and threats
- Empower junior staff to level-up by using AI to explain security alerts

Six Forces Impacting Security Decisions

Judgement is key to all great leaders and their organizations

Geo-Political

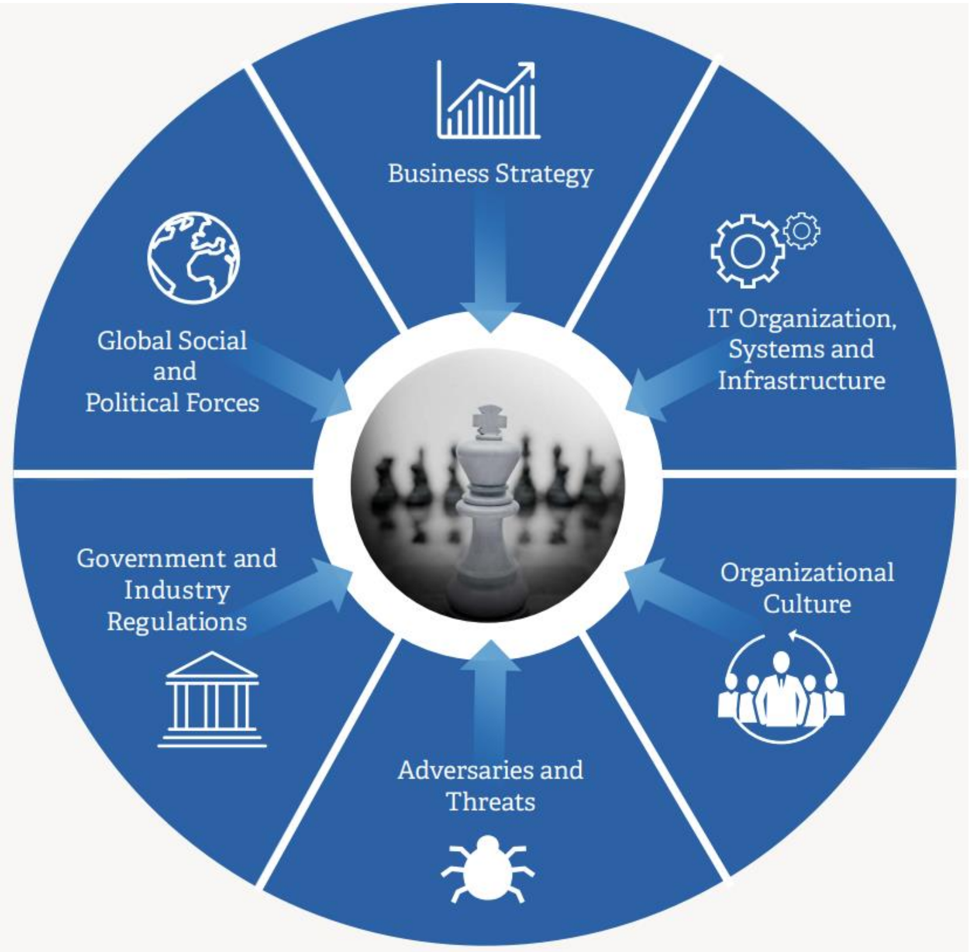
Changes in the global geo-political landscape or the global economy can have a significant impact on information security strategy.

Laws & Regulations

Must Do's, however many security programs that focus on compliance fall short of providing a framework for an effective security program.

Threats & Adversaries

Threats faced by organizations vary greatly by industry sector and are advancing every day and require consistent and continuous vigilance.



Business Strategy
IT Organization, Systems and Infrastructure
Organizational Culture
Adversaries and Threats
Government and Industry Regulations
Global Social and Political Forces

Culture

Understanding organizational bias is critical to developing
the right security strategy

Business

Whether executives are focused on growing or streamlining the business, each
carries complexities that are far different from one another

IT Strategy

The management and operation of a business's information technology systems, infrastructure and resources have a significant impact on security strategy.

Security Operations

Judgment is the key to effectiveness

1000s of hours are spent a year by organizations operating security tools

Understanding the business of security

The Business pillar defines the business objectives and management strategies of the security operations team

Interfaces – who else will be involved

The Interfaces pillar defines what functions need to be involved to achieve the stated goals. Security operations is not a silo and needs to work with many other functions of the business.

Technology – Capability Needs

element should not be thought of as a different tool but rather a capability that should be achieved with the given technology stack

People – Who will be active participants

The People pillar defines the humans who will be accomplishing the goals of the security operations team and how they will be managed

Visibility - Analyzing tons of data

What information the SecOps function needs access to. This includes security and systems data, as well as knowledge management content and communications through collaboration tools

Process and Procedures

The Processes pillar defines the processes and procedures executed by SecOps to achieve the determined mission

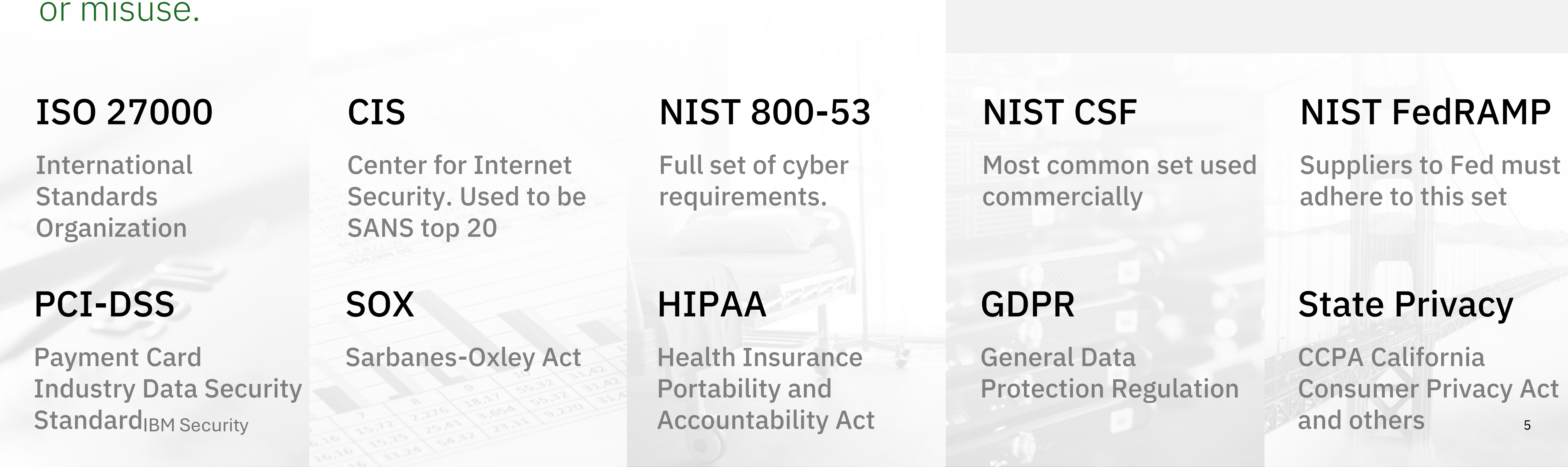
Frameworks and Compliance?

Judgment is required in how these are implemented

Frameworks - Standards and procedures with maturity expectations.

Compliance - Meeting the minimum standards required to handle regulated data with minimal risk of loss, theft, or misuse.

It is possible for an organization to model its policies based on one framework and their controls based on another.



ISO 27000

International Standards Organization

CIS

Center for Internet Security. Used to be SANS top 20

NIST 800-53

Full set of cyber requirements.

NIST CSF

Most common set used commercially

NIST FedRAMP

Suppliers to Fed must adhere to this set

PCI-DSS

Payment Card Industry Data Security Standard

SOX

Sarbanes-Oxley Act

HIPAA

Health Insurance Portability and Accountability Act

GDPR

General Data Protection Regulation

State Privacy

CCPA California Consumer Privacy Act and others

Prioritization – Competing resource demands and budgets

Judgment will be visibly on display

Audit Findings

Issues that are being tracked until completion. Often at the board level through the Audit Committee

The 3 R's

What makes you rich
What will ruin you
What is required

Risk

Risk mitigation not risk elimination. Risk is a key business element, without it there are no returns

CIA Triad

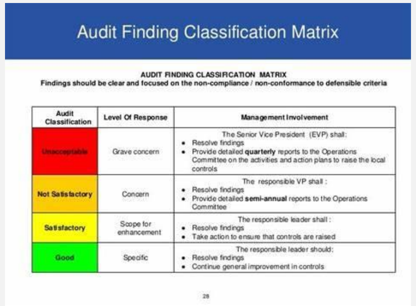
Loss of:
- Confidentiality
- Integrity
- Availability

CIA Extended

Must assure:
- Authenticity
- Accountability
- Non-repudiation

The Box -

Every security team is in box and allowed to operate within certain boundaries that impact the strategy.



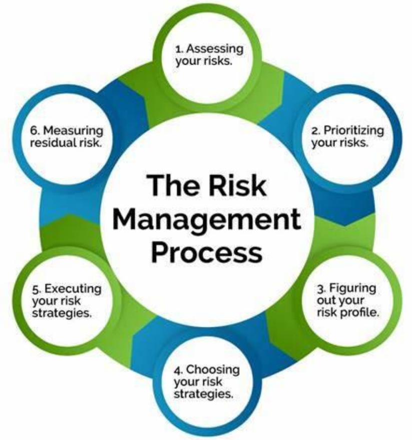
Audit Finding Classification Matrix

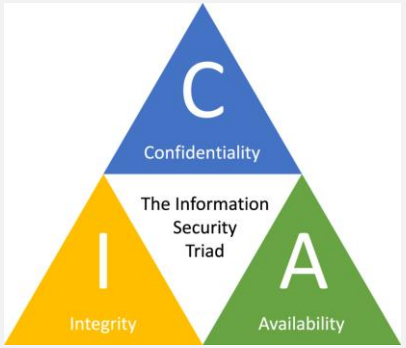
AUDIT FINDING CLASSIFICATION MATRIX
Findings should be clear and focused on the non-compliance / non-conformance to defensible criteria

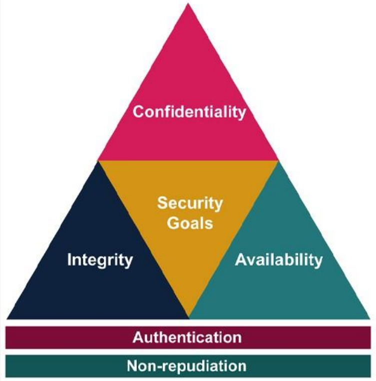
Audit Classification	Level Of Response	Management Involvement
Unacceptable	Grave concern	The Senior Vice President (EVP) shall: • Resolve findings • Provide detailed **quarterly** reports to the Operations Committee on the activities and action plans to raise the local controls
Not Satisfactory	Concern	The responsible VP shall : • Resolve findings • Provide detailed **semi-annual** reports to the Operations Committee
Satisfactory	Scope for enhancement	The responsible leader shall : • Resolve findings • Take action to ensure that controls are raised
Good	Specific	The responsible leader should: • Resolve findings • Continue general improvement in controls

28

IBM Security


The Risk Management Process
1. Assessing your risks.
2. Prioritizing your risks.
3. Figuring out your risk profile.
4. Choosing your risk strategies.
5. Executing your risk strategies.
6. Measuring residual risk.


C
Confidentiality
The Information Security Triad
I
Integrity
A
Availability


Confidentiality
Security Goals
Integrity
Availability
Authentication
Non-repudiation