Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Advanced Security (Information Security Management) Session 2: Information Security Frameworks and IS Organizations

Prof. Dr.-Ing. Sebastian Schlesinger
Professor of Business Computer Science
(Security and Embedded Systems Engineering)

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Goals of the Lecture

- Setting the Scene: IS in the context of companies
- Clarify some basic vocabulary
- Getting first insights to IS compliance frameworks

Introduction

Organizations of all types and sizes:

- collect, process, store, and transmit information
- recognise that information, and related processes, systems, networks and people are important assets for achieving organization objectives
- Face a range of risks that can affect the functioning of assets
- Address their perceived risk exposure by information security controls

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

What is a Risk?

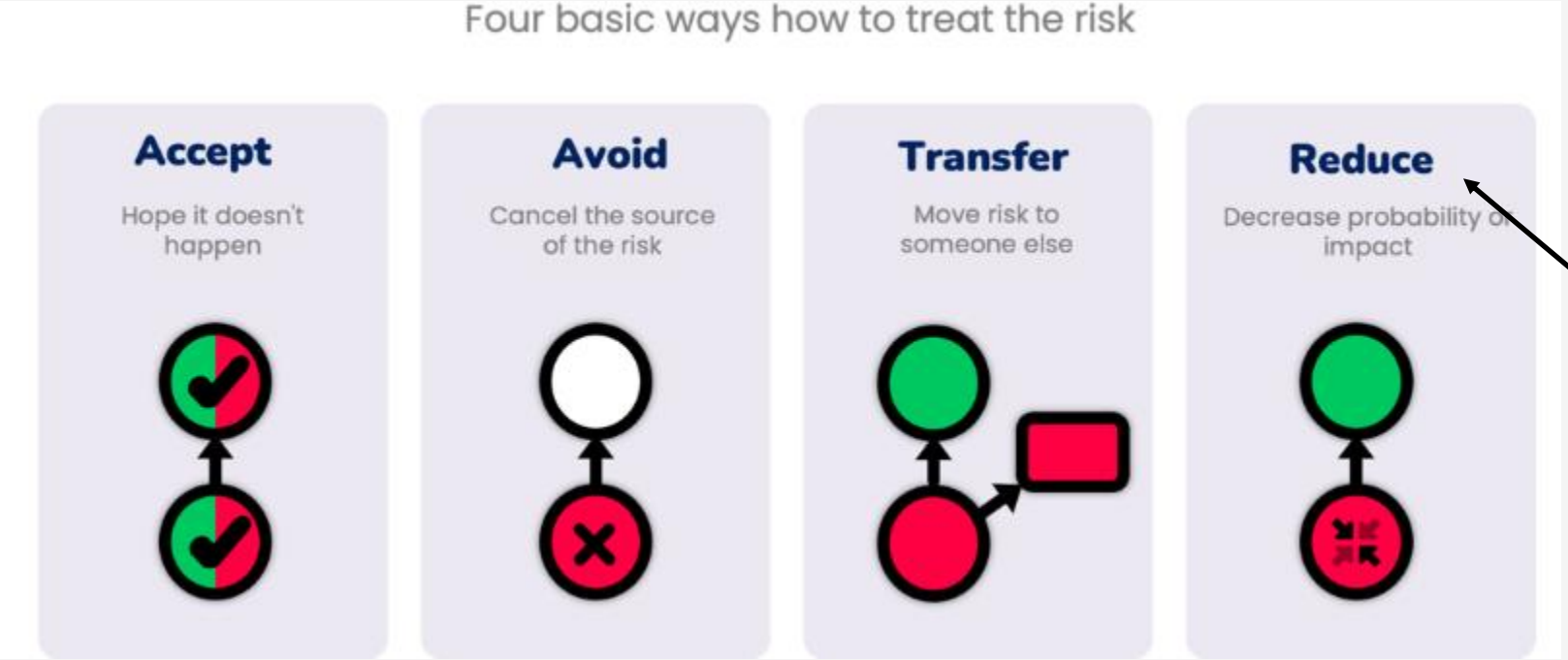
The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Source: NIST glossary

Risk Treatment Strategies

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



often referred to as „mitigate“

Source: https://aptien.com/en/kb/articles/what-are-risk-treatment-strategies

Risk Management Cycle

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

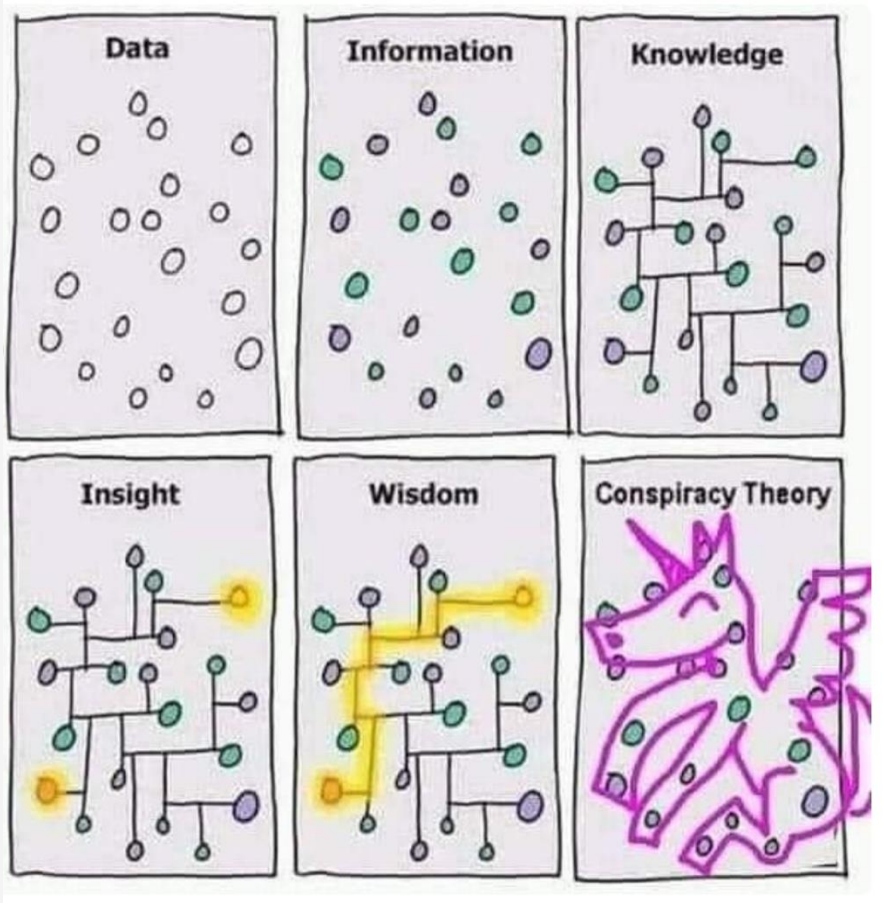
Source: https://www.cascade.app/blog/risk-mitigation-strategies

Risk Types

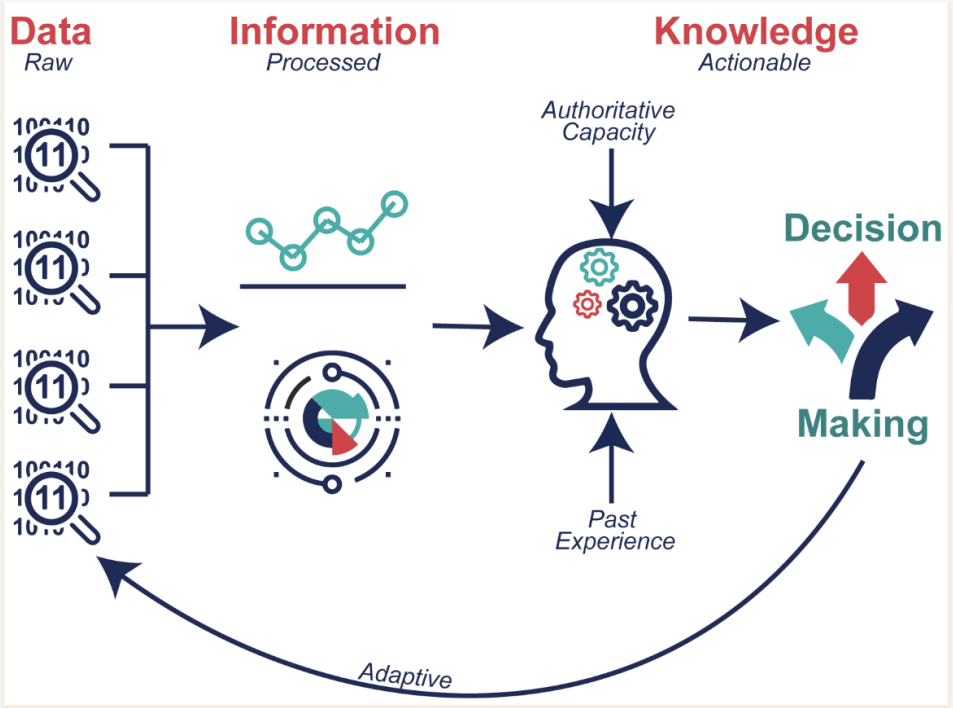
Source: https://www.cascade.app/blog/risk-mitigation-strategies

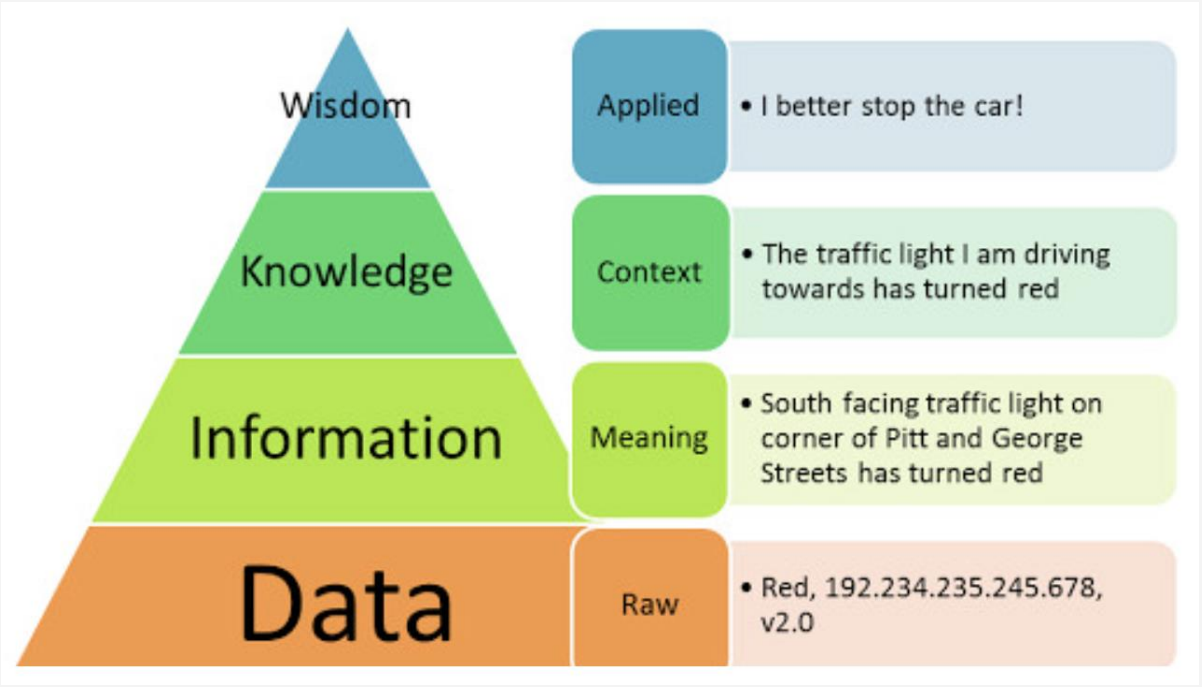
What is information?

- Information is processed data that holds meaning and value
- It is essential for decision-making, communication, and operations
- Example: Personal data, financial records, intellectual property.



Other Perspectives on Information





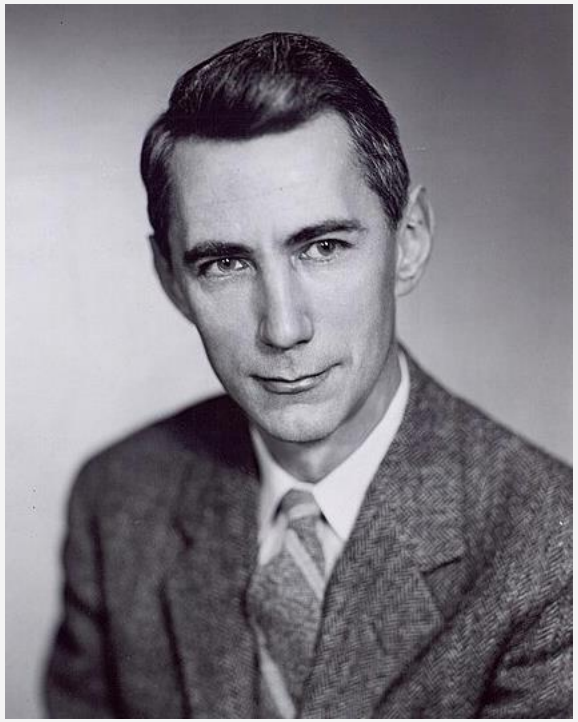
Sources: https://oddur-bjarnason.org/the-data-information-knowledge-process/, https://www.linkedin.com/pulse/20140722053326-3033591-the-journey-from-data-to-knowledge-and-wisdom/

Another Perspective on Information: Information Theory

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Entropy: In information theory, the amount of uncertainty or unpredictability in a message is measured by a concept called **entropy**.

$$H(X) = -\sum_{i=1}^{n} p(X = x_i) \log_2 p(X = \mathrm{x}_i))$$



The information content or **self-information** of a specific event or symbol is defined as the negative logarithm of its probability. Rare events have higher information content because they reduce more uncertainty when they occur.

$$I(x_i) = -\log_2 p(x_i)$$

Question

What kind of information would you consider protect-worthy in a company context?

Why Information needs Protection?

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Can you imagine main reasons for the need to protect information?

Threats to IS (extract)

- **Cyber Attacks:** Hacking, malware, phishing
- **Insider Threats:** Employees or insiders misusing access
- **Physical Theft:** Stealing hardware or devices containing sensitive information
- **Human Error:** Accidental data breaches or improper handling of information.

Protection Goals for Cybersecurity

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

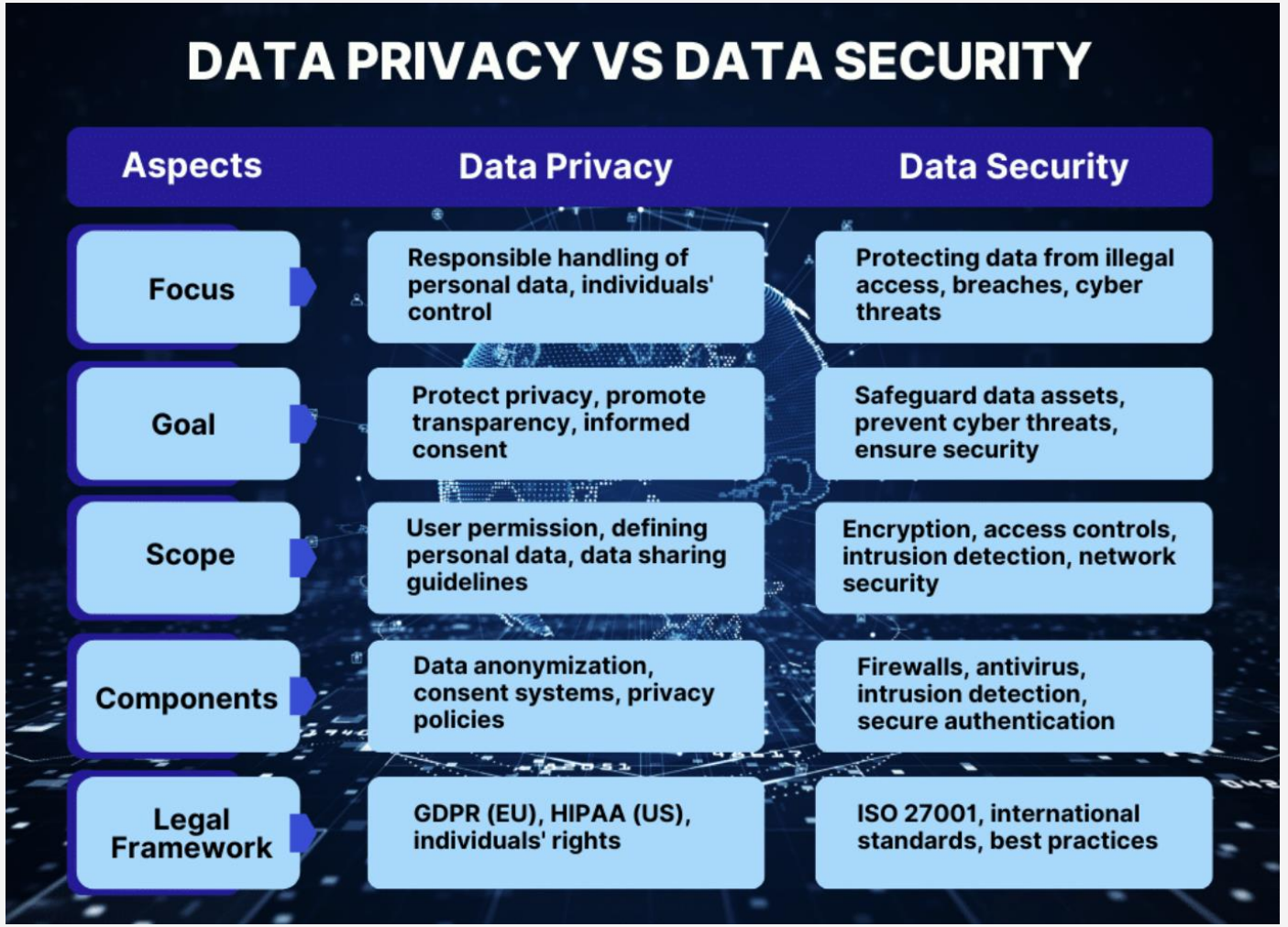
Role of Information Security in a Wider Context

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Try to define the terms and distinguish between them!

Also, what is the difference between privacy and security? (Next slide)

Information Security vs. Privacy



Source: https://www.redswitches.com/blog/data-privacy-vs-data-security/

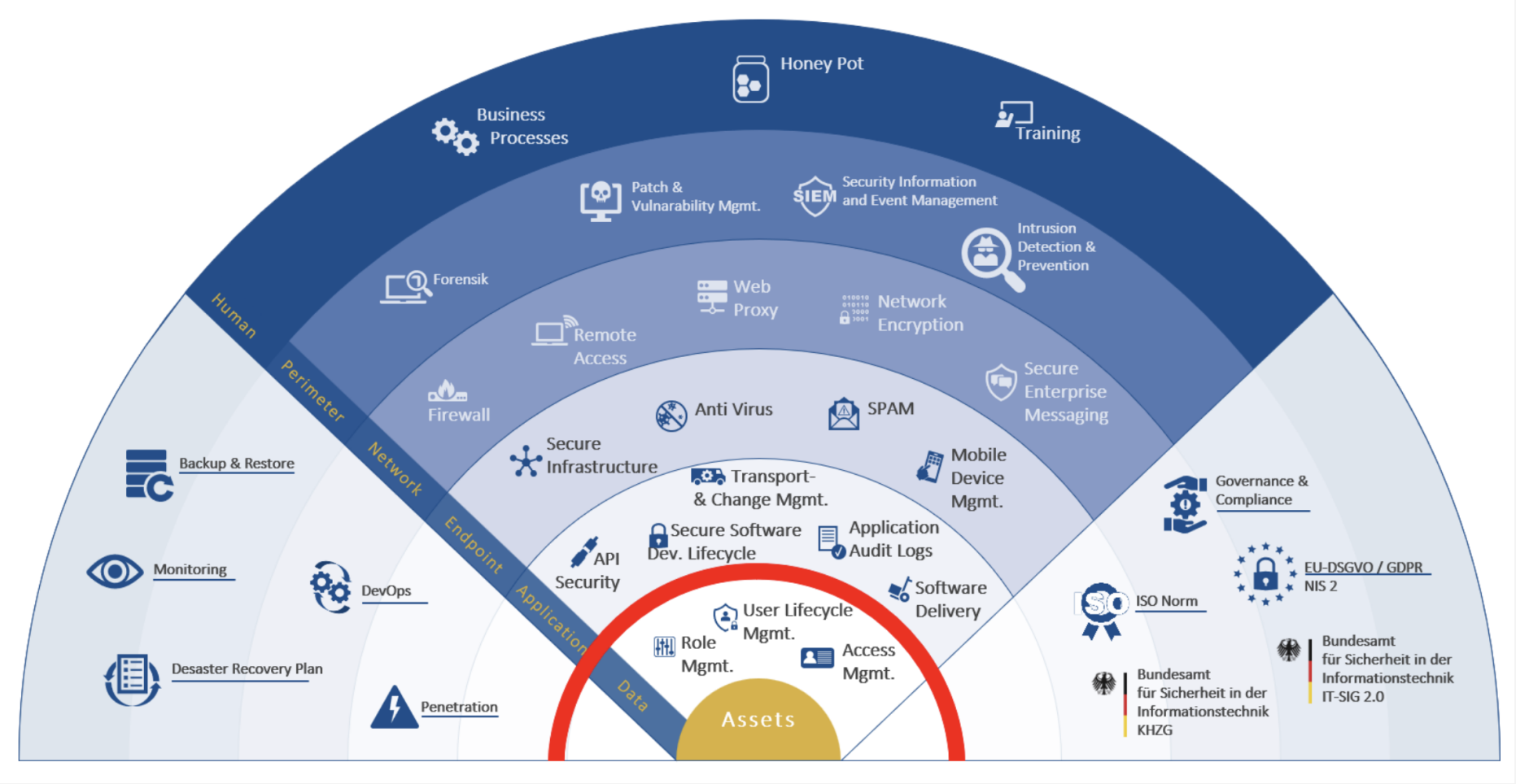
Question

Can you imagine some challenges to ensure information security in a company context?

What kind of tasks would you consider to be relevant for the cybersecurity domain in a company?

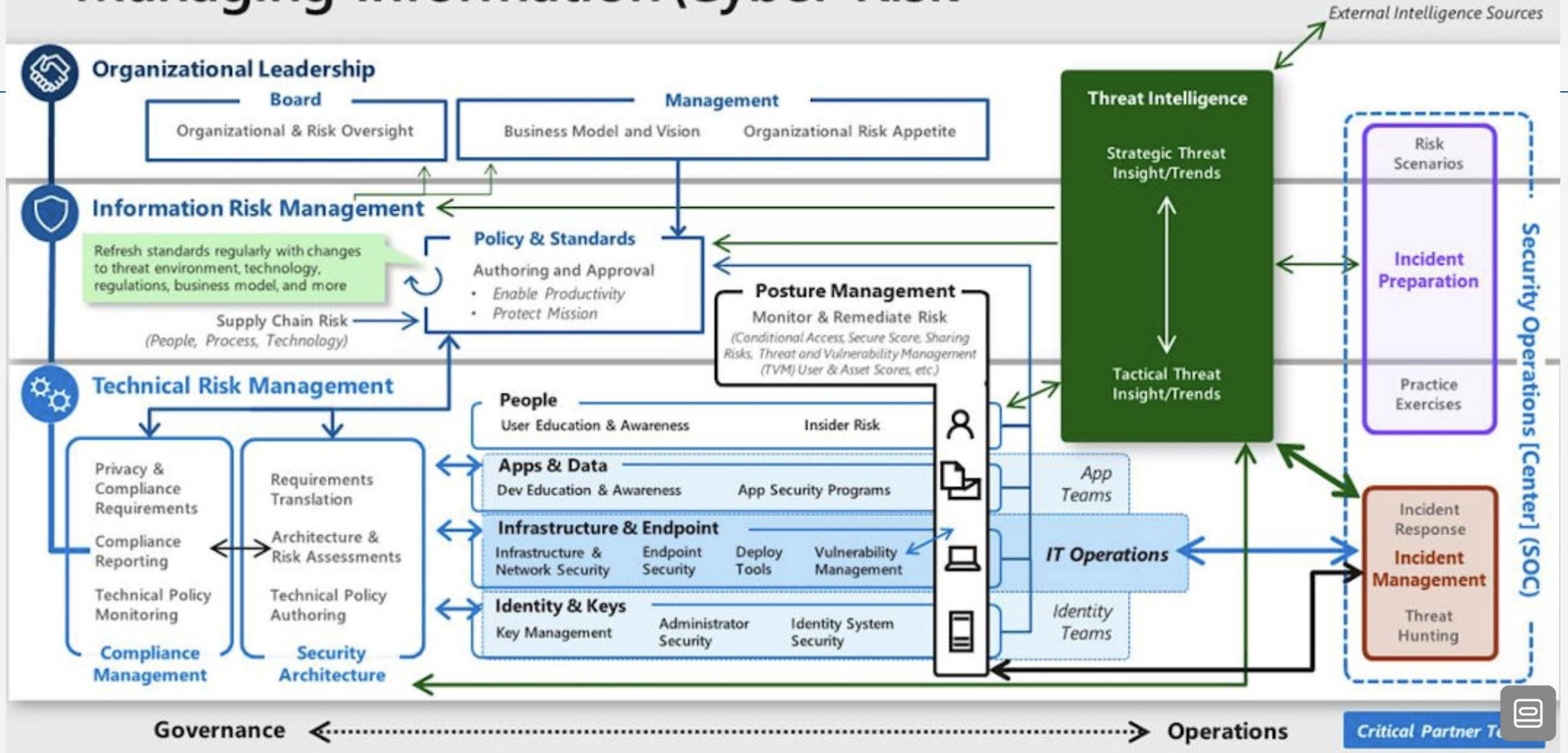
Some Tasks Relevant for Cybersecurity Department

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Source: https://www.ibsolution.com/academy/blog_en/cyber-security/nis-2-what-companies-must-do-for-their-cyber-security

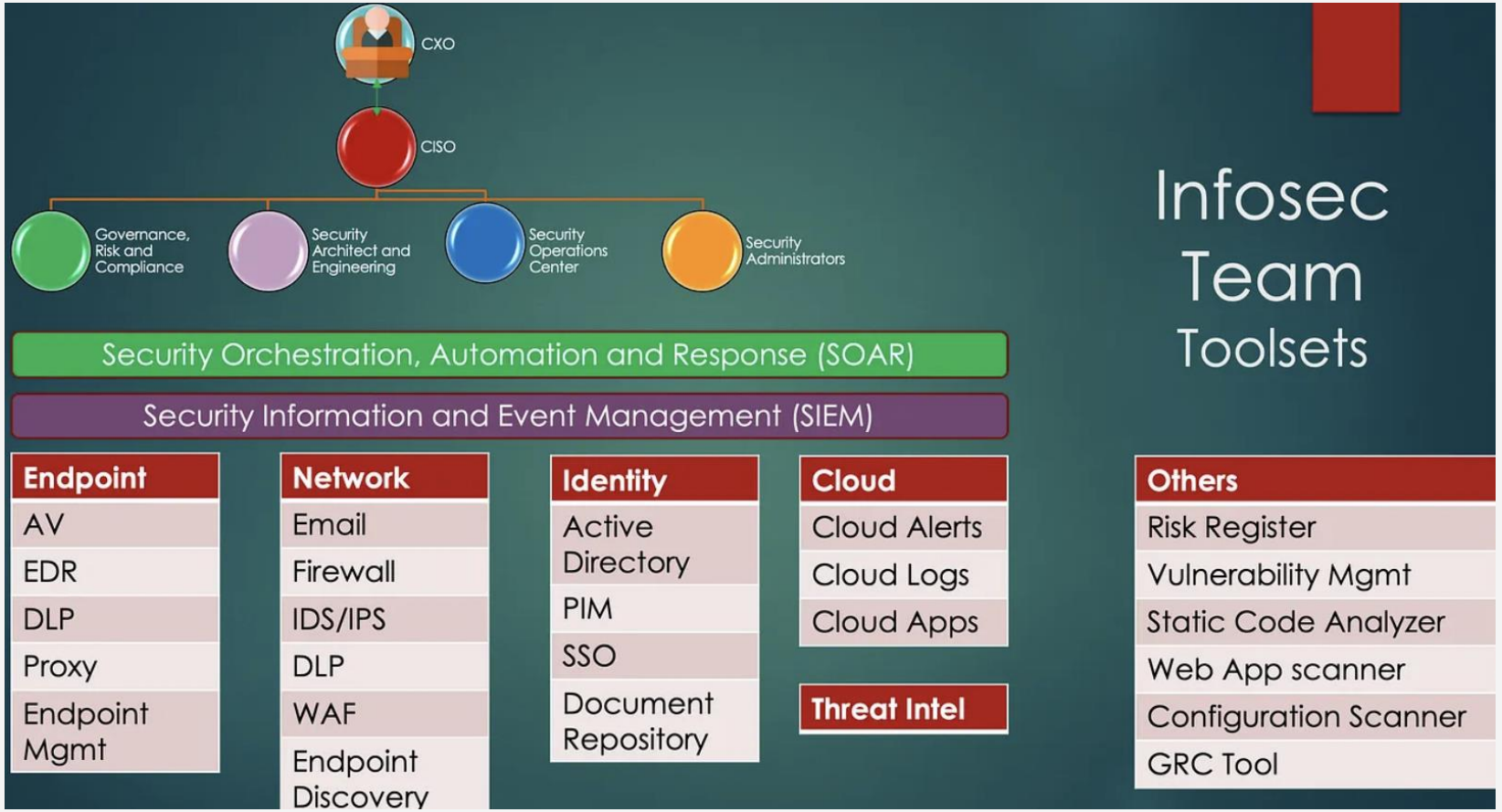
Managing Information\Cyber Risk



Source: https://spin.ai/blog/cyber-security-roles-responsibilities-enterprise/

Cybersecurity Organizations

- Chief Information Security Officer (CISO)
- Security Operations Center (SOC)
- Identity and Access Mangement (IAM)
- Compliance / Trust & Assurance
- Product / Application Security
- …



Source: https://medium.com/@inishantgrover/information-security-governance-risk-and-compliance-team-5b7222f12f21

Some Roles in Cybersecurity Organizations

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Chief Information Security Officer (CISO)
- Software Engineer
- Security Engineer
- Product / Application Security Experts
- Rapid Responder
- Security Architect
- Security Analyst
- Forensic Specialists
- Auditors
- Compliance Managers
- …

Try to guess what the responsibilities of those roles are and where they are

Operational Security in Company Context

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Do you know some tools to support cybersec?

Some Key Tools for Cybersecurity

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

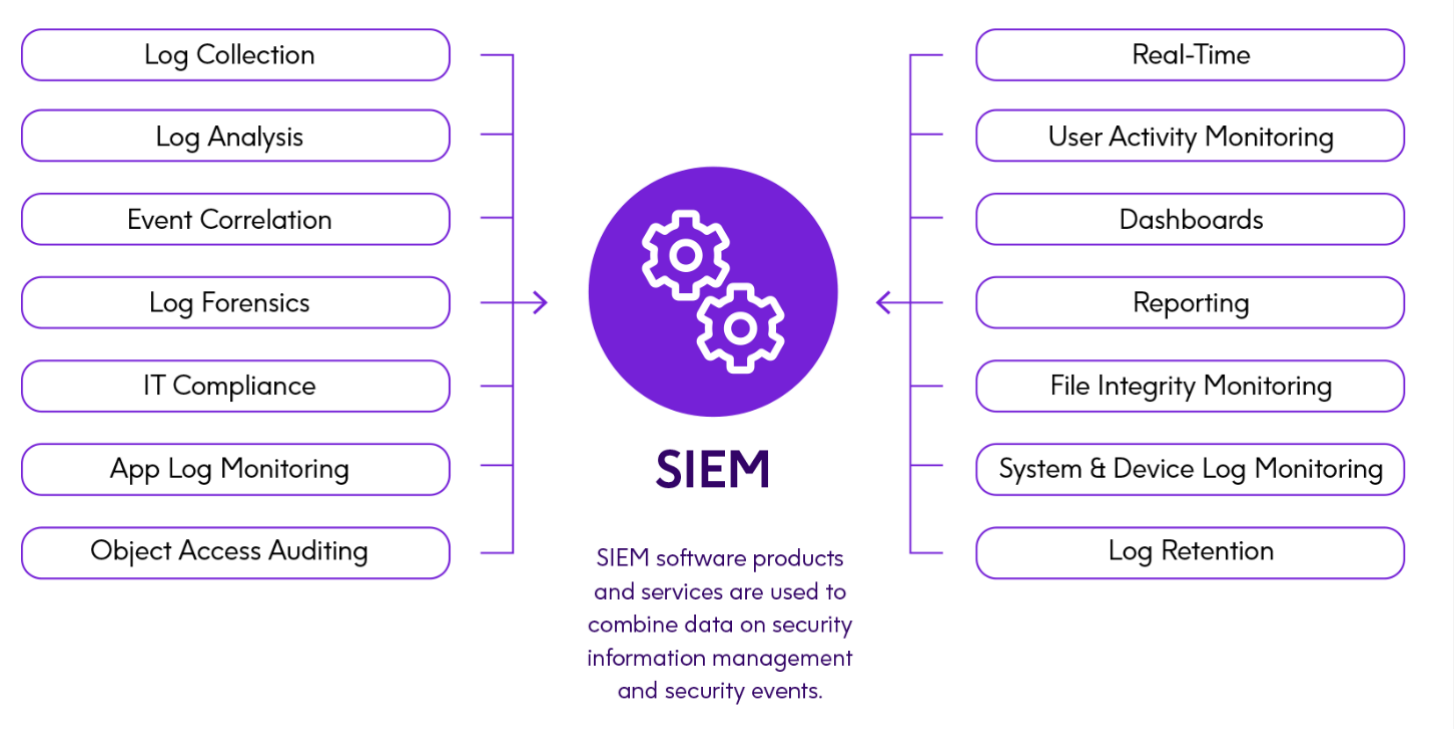
- Security Information and Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)
- Security Orchestration, Automation, and Response (SOAR)
- DDoS Prevention
- Firewalls
- Vulnerability Management Tools
- Threat Intelligence Platforms (TIPs)
- Network Traffic Analysis Tools (NTA)
- Data Loss Prevention (DLP)
- IAM Tools
- Penetration Testing Tools
- Web Application Firewalls (WAF)
- Encryption Tools
- Backup and Recovery Tools

SIEM Systems

Key Features

- Real-time monitoring
- Event correlation
- Log management
- Incident detection and response

Examples: Splunk, IBM QRadar, ArcSight, LogRhythm.



Source: https://www.precisely.com/de/solution/loesungen-fuer-security-information-and-event-management-siem

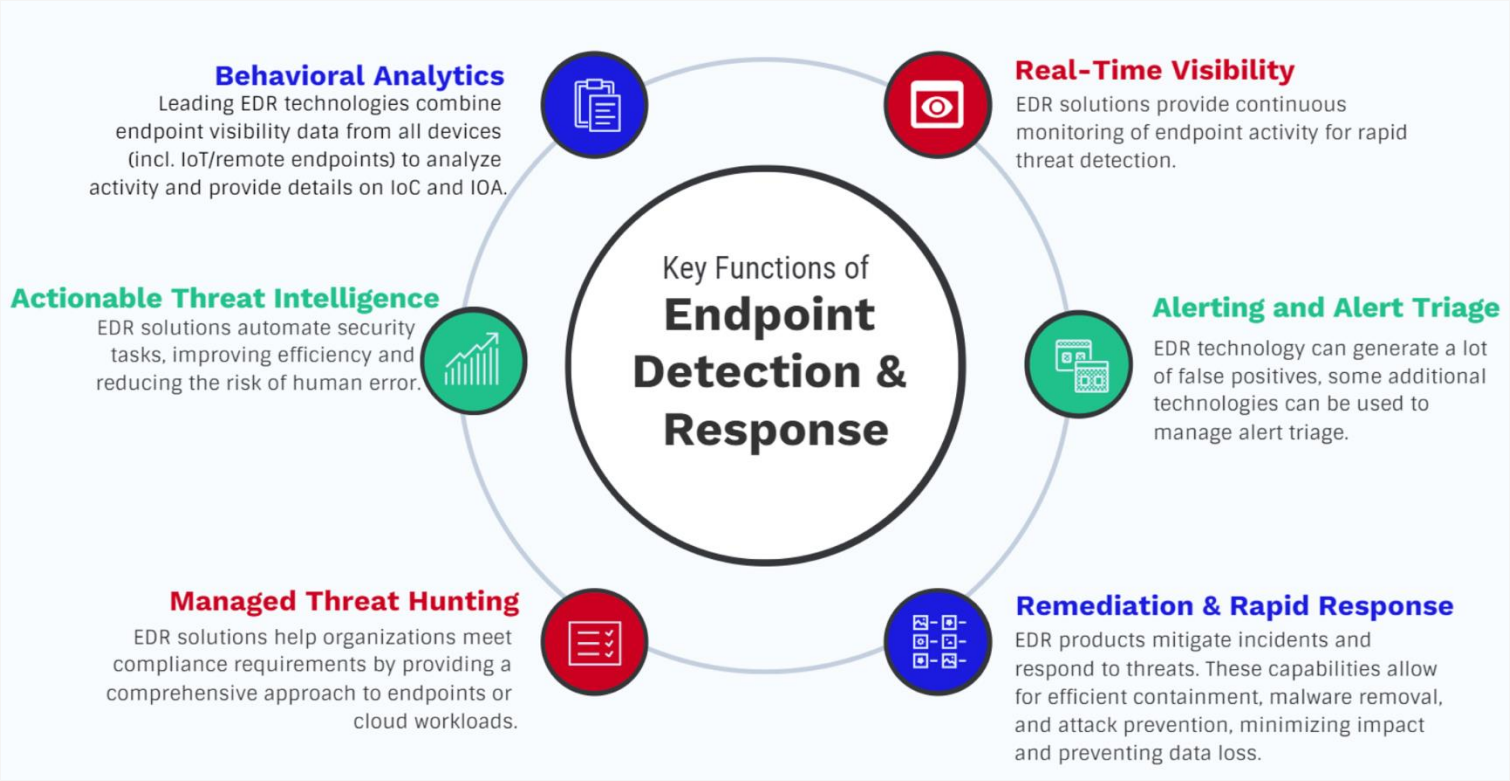
Endpoint Detection and Response (EDR) Systems

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- To protect endpoints (APIs)

Key features
- Real-Time Continuous Monitoring
- Endpoint Data Collection
- Automated response (rule-based / AI-based)

Examples: VMWare Carbon Black, CrowdStrike Falcon, Akamai API Security



Source: https://www.openedr.com/blog/what-is-edr/

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

IDS / IPS Systems

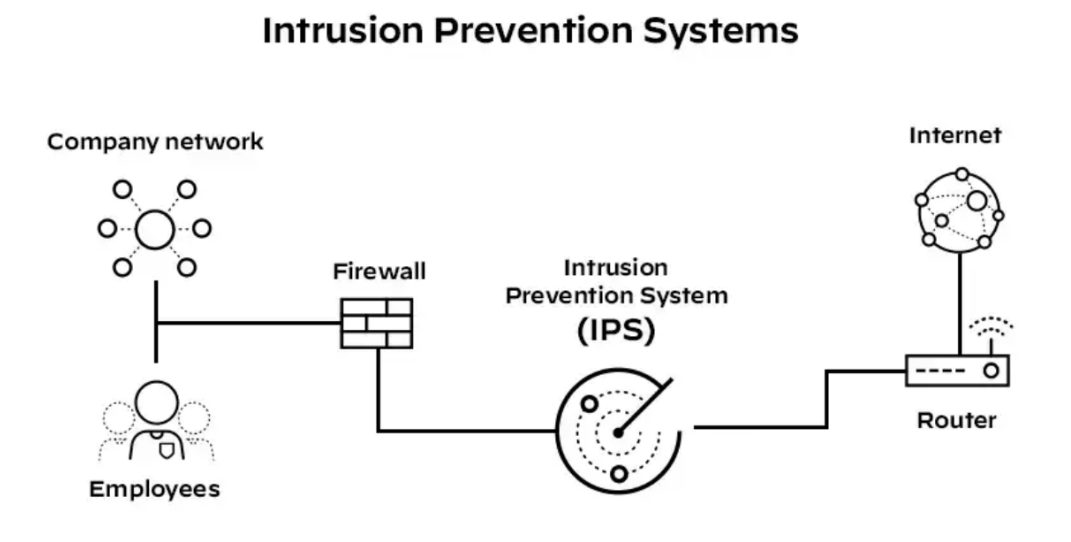
IDS Features

- **Log Analysis:** Scrutinizing system logs to identify patterns indicative of potential security breaches.
- **Real-Time Monitoring:** Continuous monitoring of network traffic for immediate threat detection.
- **Alerts and Notifications:** Promptly notifying administrators of suspicious activities for swift response.

IPS Features

- **Firewall Integration:** Seamlessly integrating with firewalls to enhance preemptive security measures.
- **Policy-Based Blocking:** Applying predefined policies to automatically block malicious activities.
- **Anomaly Detection:** Identifying deviations from normal network behavior and taking preventive actions.

Examples: Palo Alto Networks, Check Point Quantum IPS, Zscalar Cloud IPS, Kismet, Cisco NGIPS



Source: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

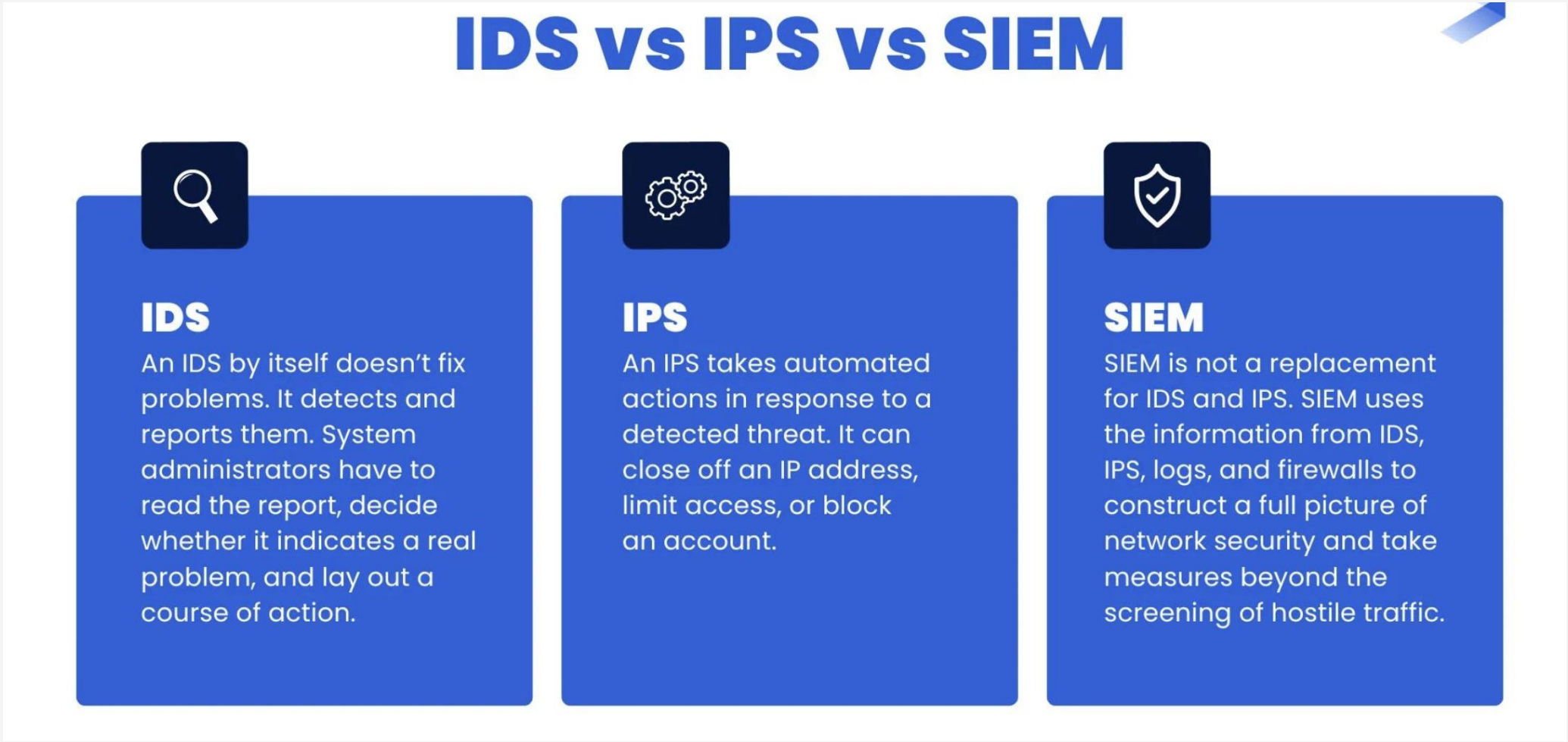
Task

Can you imagine some patterns that may be recognised by an IDS that indicate spurious behavior?

Try to differentiate SIEM, EDR, IDS/IPS systems from each other.

Differentiation of the systems we encountered so far

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Source: https://www.bitlyft.com/resources/ids-vs-ips-vs-siem

Security Orchestration Automation and Response (SOAR)

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Closely related with SIEM
- In a view SIEM on a larger scale
- Focus on top attack vectors and orchestration around that
- Higher-order inference on lower-level observations
- Tools and culture / approach

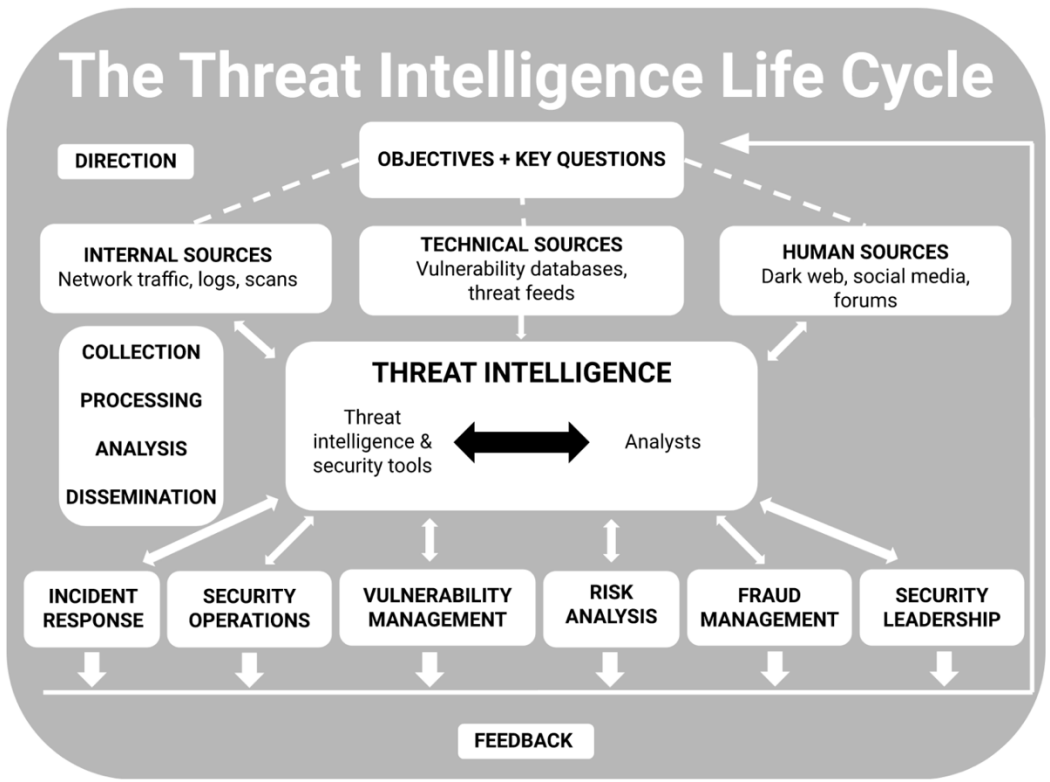
Examples: IBM Qradar, ServiceNow, Splunk, Fortinet

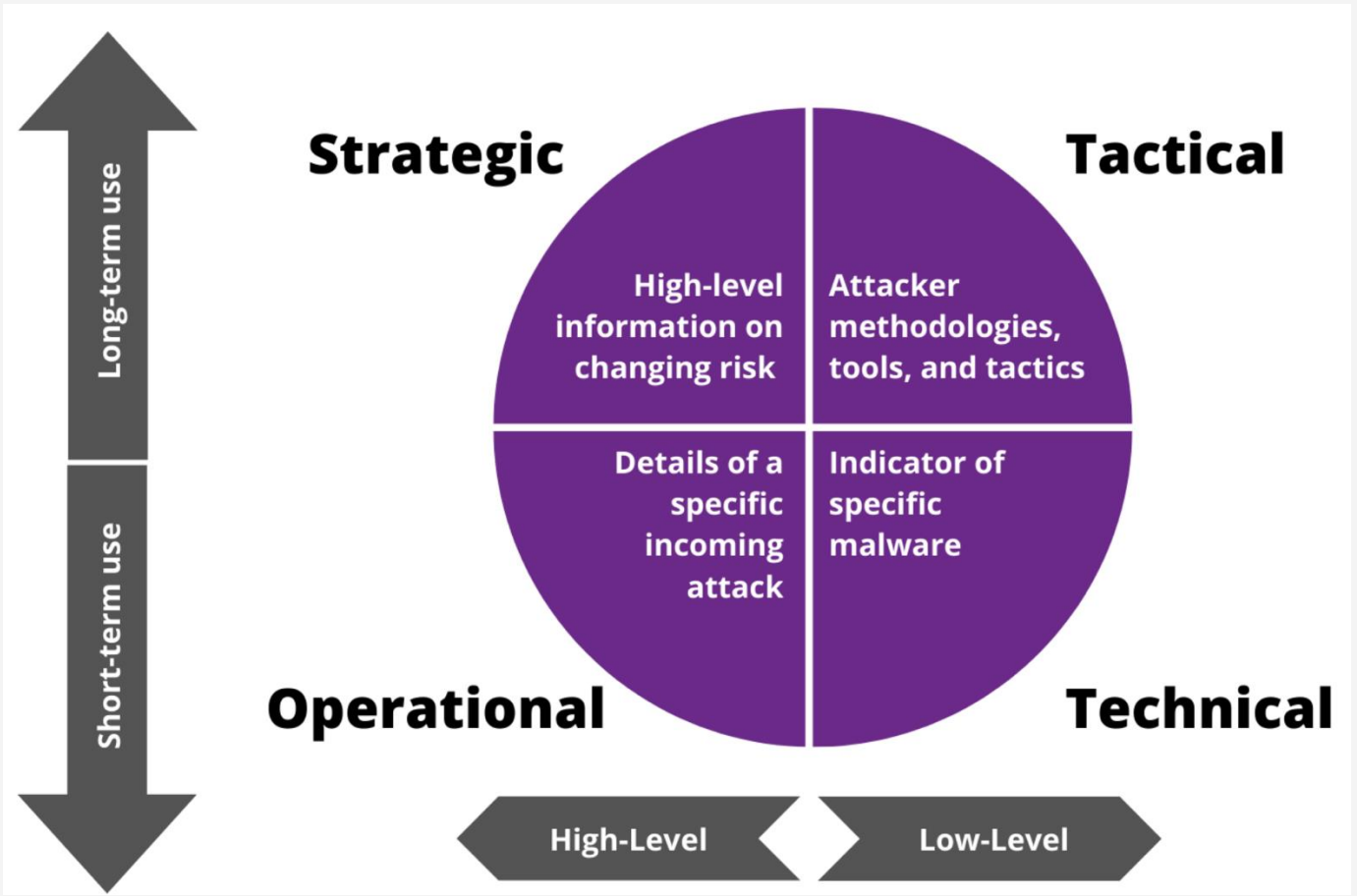
Exercise: Splunk → https://docs.splunk.com/Documentation/SOAR
Register for test account, generate sample log data via ChatGPT, ingest it and analyse it

Source: https://medium.com/@cloud_tips/soar-security-orchestration-automation-and-response-definition-best-practices-and-tools-8a20dd590bd5 , https://www.office1.com/blog/what-is-soar-and-how-can-it-help-my-enterprise

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Threat Intelligence



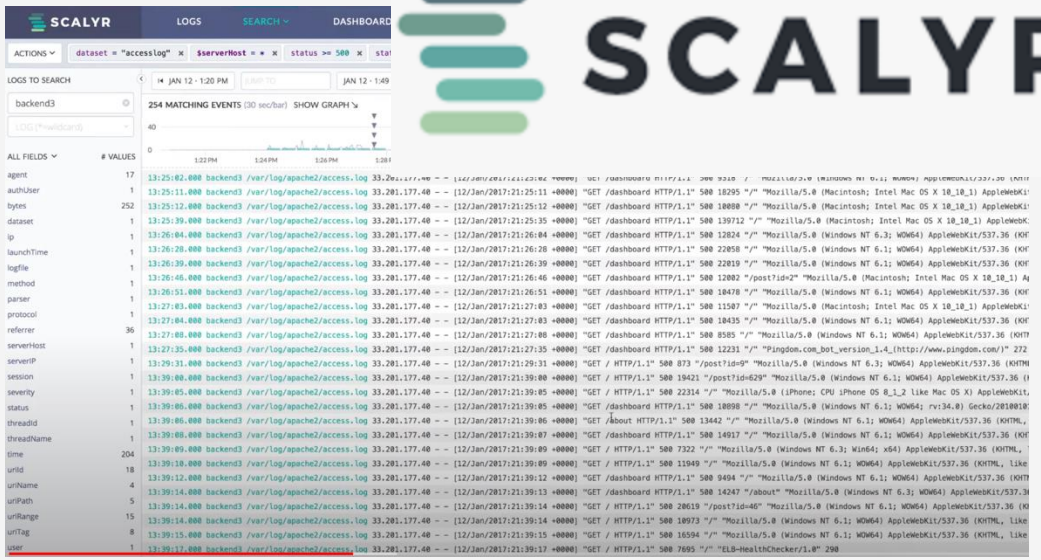


Examples: ThreatConnect, Rapid7 Threat Command, Palo Alto Networks Cortex XSOAR

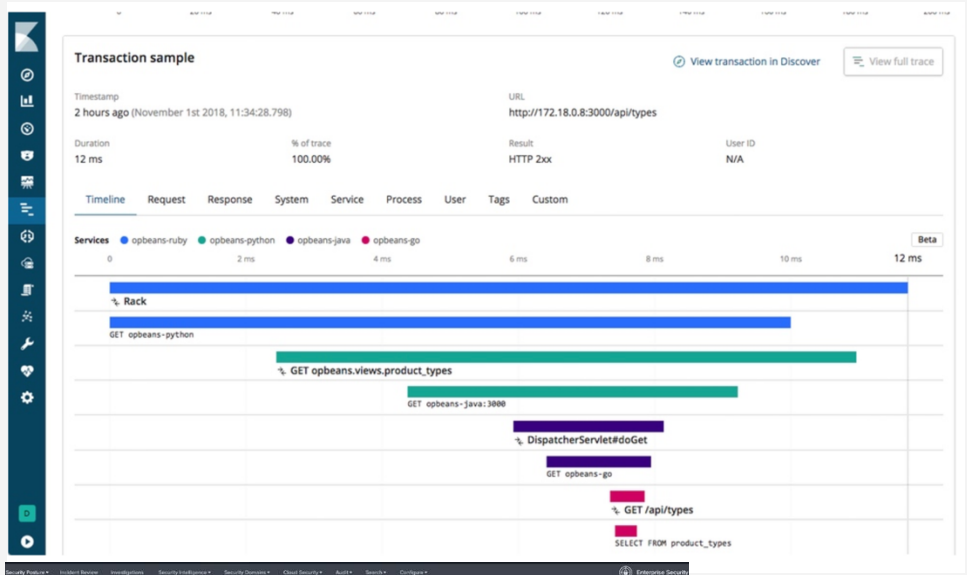
Source: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-threat-intelligence/ https://www.balbix.com/insights/cyber-threat-intelligence-guide/

Forensics

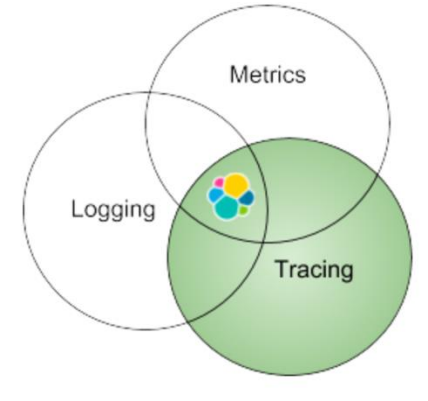
Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



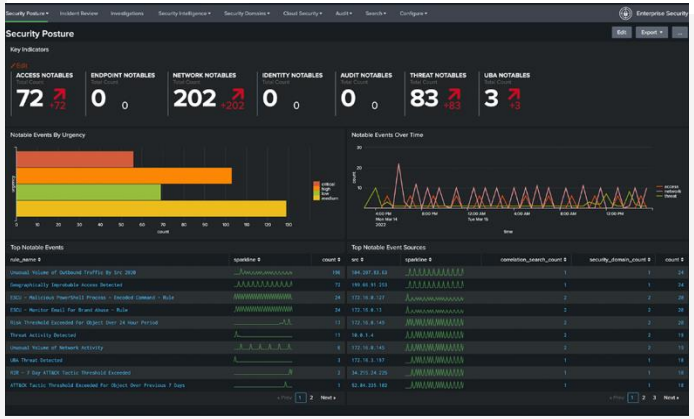
SCALYR



What to consider when enabling forensics?



OPEN TRACE

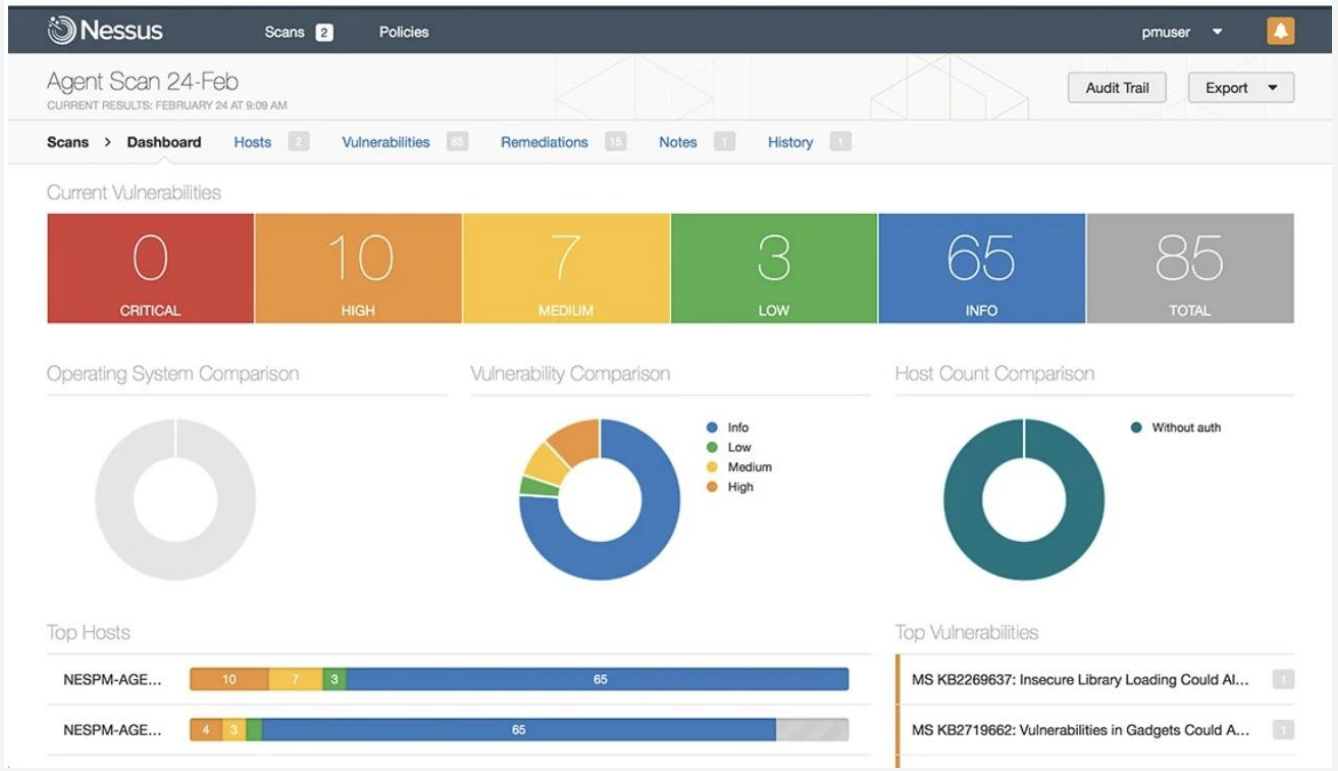


splunk>

Question

- Where do you see the challenges in implementing such a system (comprising EDR, IPS, SIEM, SOAR, Threat Intelligence)?
- How could steps be to implement such systems? How would you tackle the problem?
- What to consider?

Asset Management and Scanning

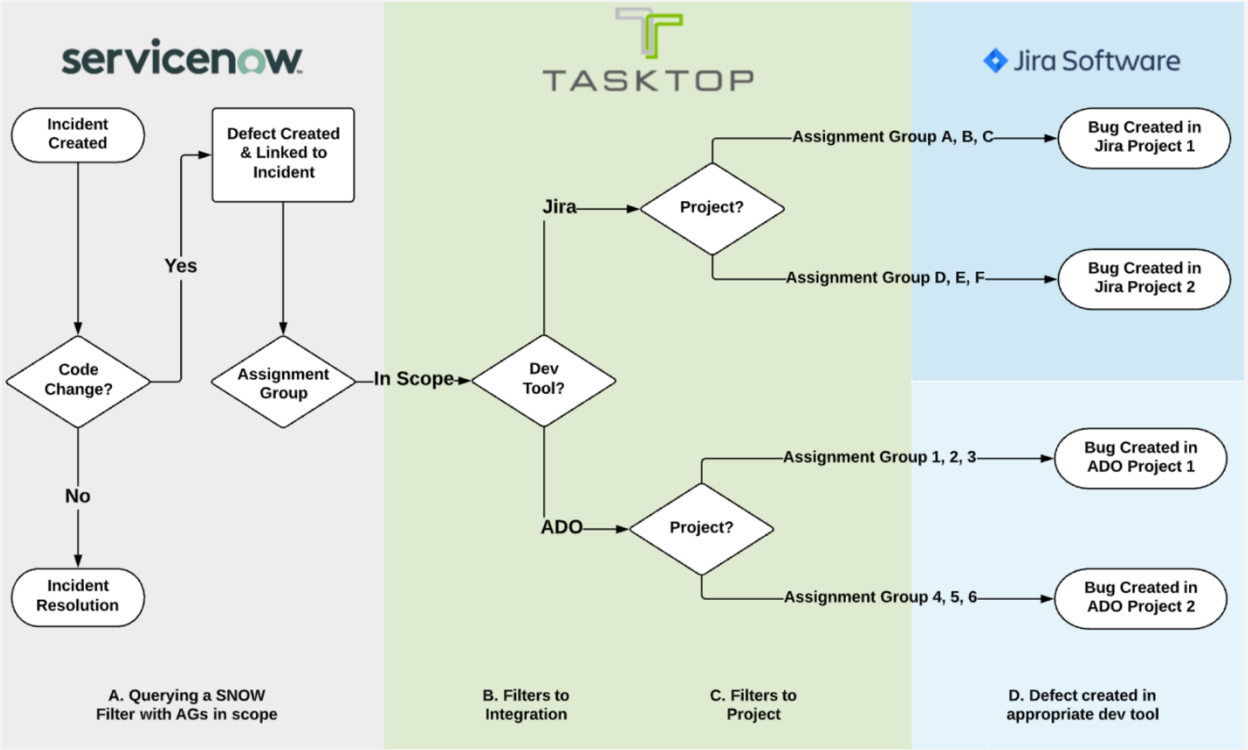


- Regular Scanning for changes in the infrastructure
- Internal and external posture
- Asset Management: Inventory of assets together with meta info and classifications

Questions

- Why is asset management and scanning important?
- What are challenges around that?

Incident Management



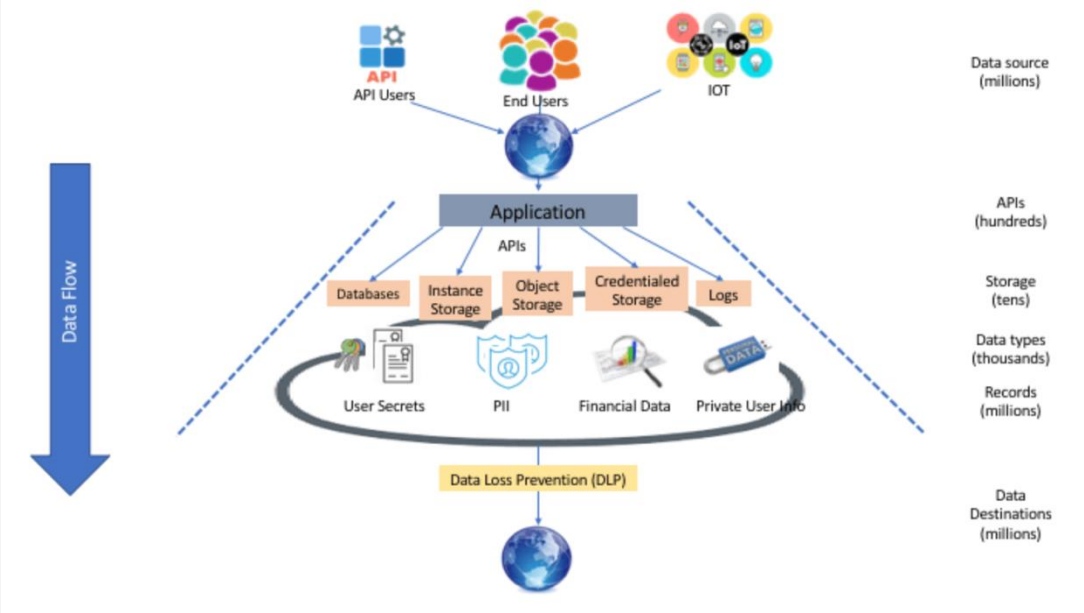
- Operational Excellence
- Focus at Web: MTTR prio (vs. MTBF focus)
- Entails rapid response, forensics
- Operational Excellence Meetings

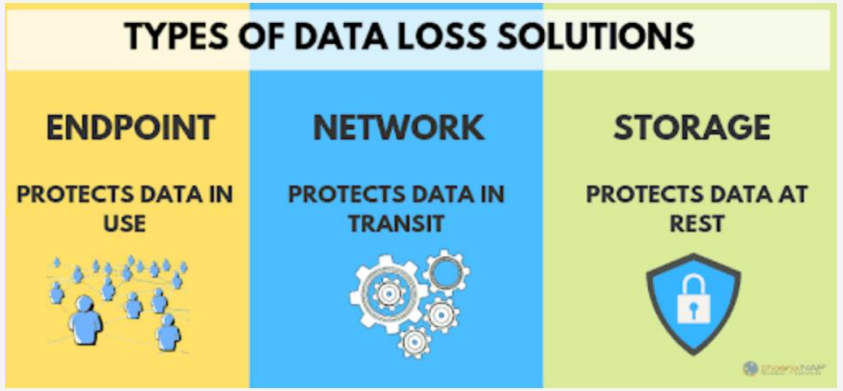
Question

- What challenges do you expect?

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Data Loss Prevention





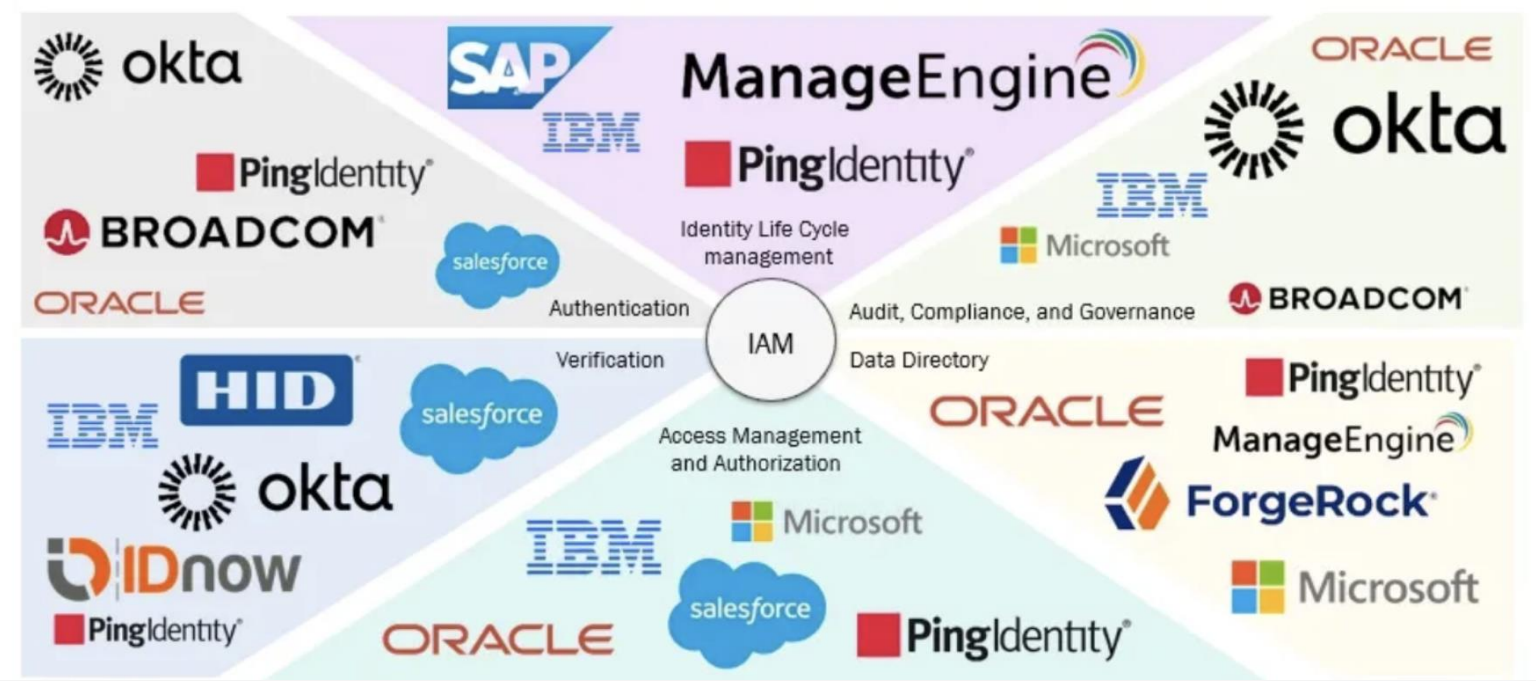
Examples: Digital Guardian, BetterCloud, Endpoint Protector, Broadcom Symantec DLP, Check Point

Source: https://www.linkedin.com/pulse/data-leakage-prevention-dlp-steps-strategies-bizcomglobal-2he2c/ https://cyberready.com/de/the-infosec-guide-to-data-loss-prevention/top-9-data-loss-prevention-dlp-tools

IAM Tools

Some tasks around IAM

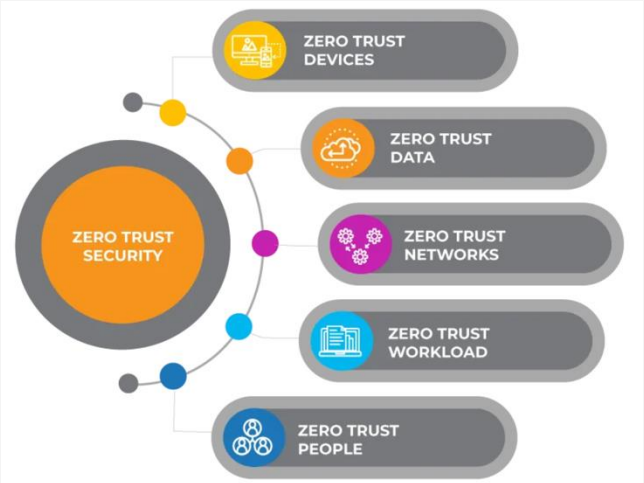
- User provisioning, life cycle management
- Authentication, SSO
- Authorization, access control
- MFA
- Privileged Access Management
- Auditing & Compliance

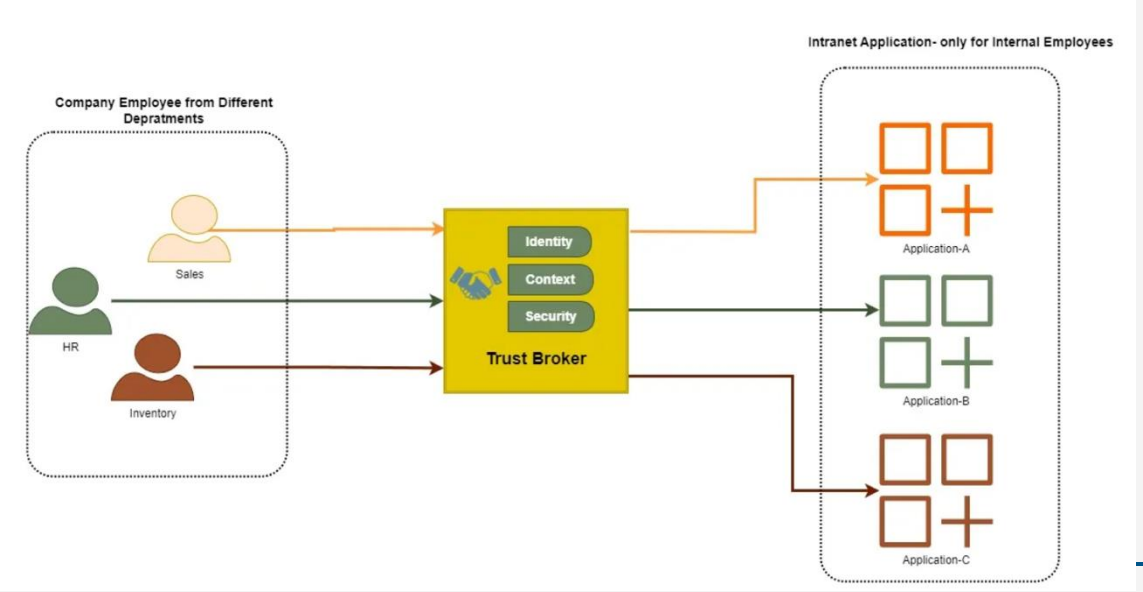


Source: h https://medium.com/@hildamachando4/a-journey-into-the-realm-of-iam-an-introduction-to-the-cutting-edge-solutions-in-the-market-eb7c63bc1fad

Zero Trust Approach

- No user or device can be trusted by default (no one outside or inside the network unless authenticated)
- Need to know principle, least privilege principle
- Verification via identity, context, security posture of connecting device (compliance)



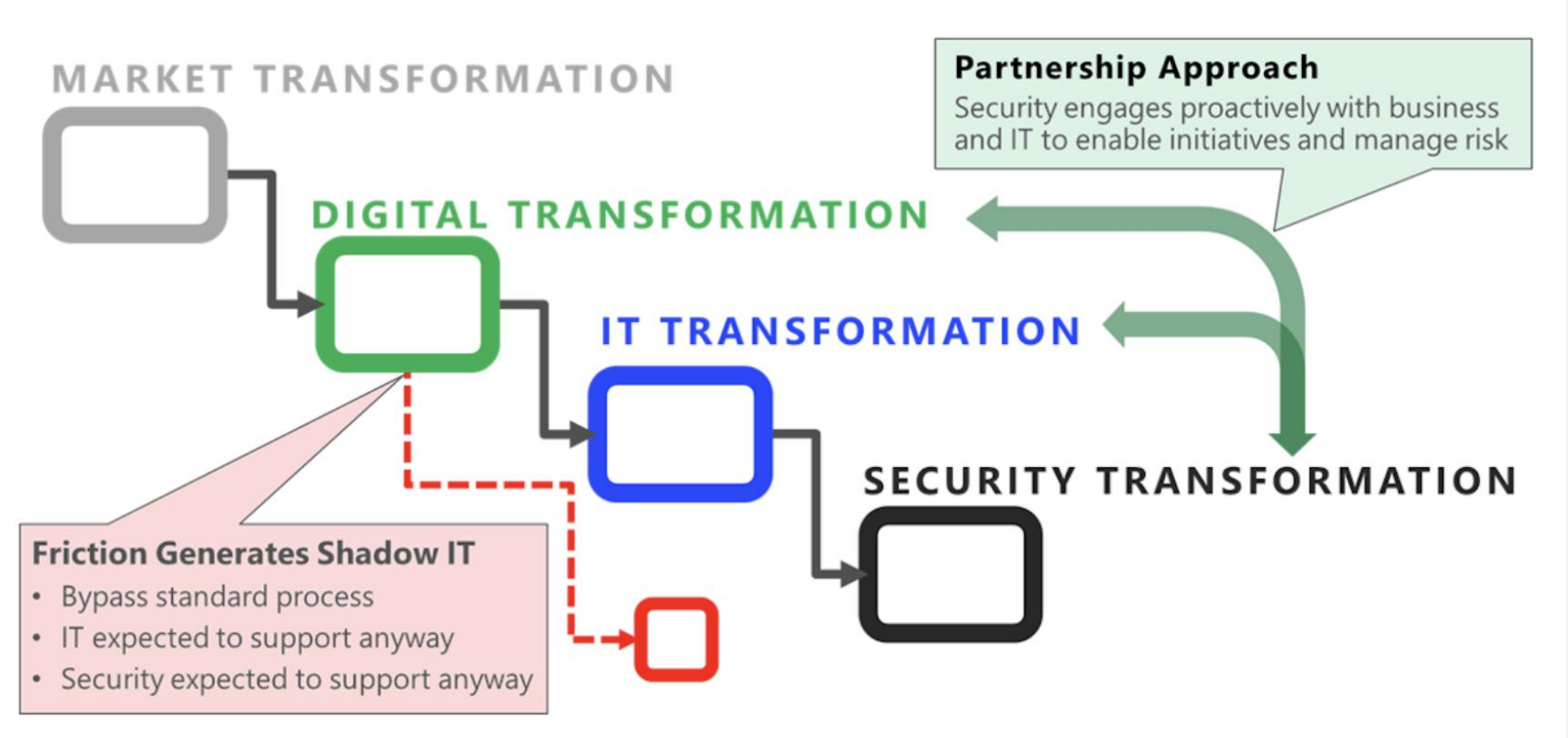


Source: https://medium.com/google-cloud/zero-trust-security-model-a-new-approach-to-network-security-9dee89564b3e

Question

We took a look at a standard IS organization. However, key is the entanglement with business.
Why?
How can that be achieved?

Challenges for Security in Organizations



Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/define-security-strategy

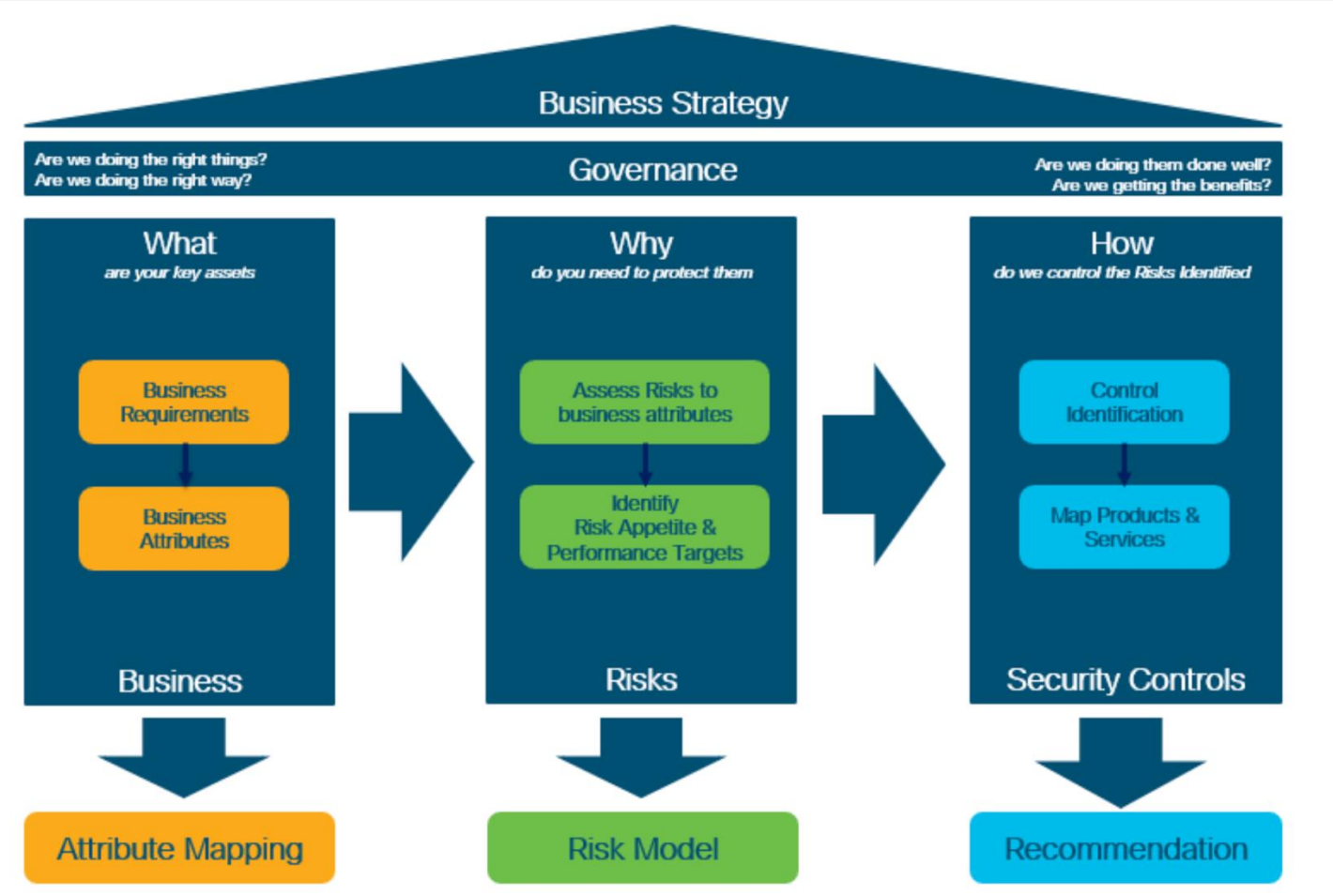
Derive a Security Strategy from the Business Strategy

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Source: https://deltalogix.blog/en/2022/09/14/cybersecurity-strategy-what-are-the-key-aspects-to-consider/

Derive a Security Strategy from the Business Strategy

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Source: https://gblogs.cisco.com/uki/business-driven-information-security-part-3/

Why is it important to balance business strategy and security strategy?

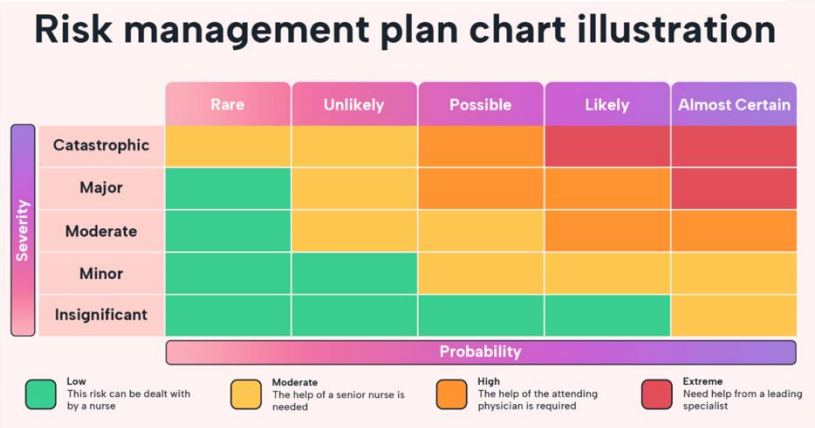
Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Source: https://citysecuritymagazine.com/risk-management/opinion-corporate-security-strategy-3/

Some related strategic terms

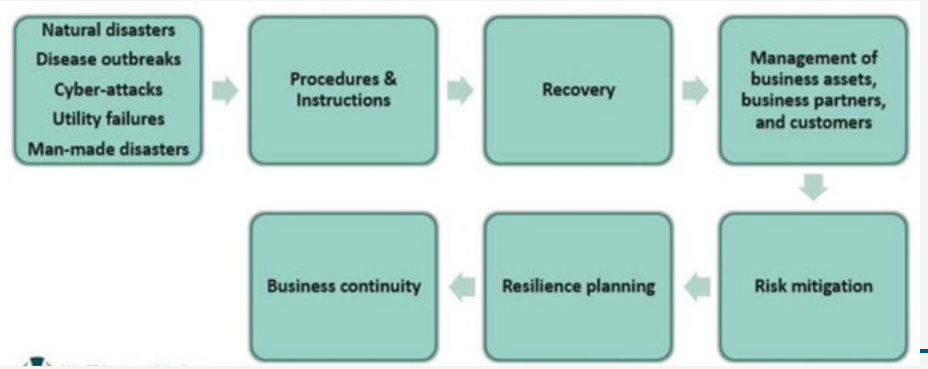
Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Risk Management



Business Continuity Management

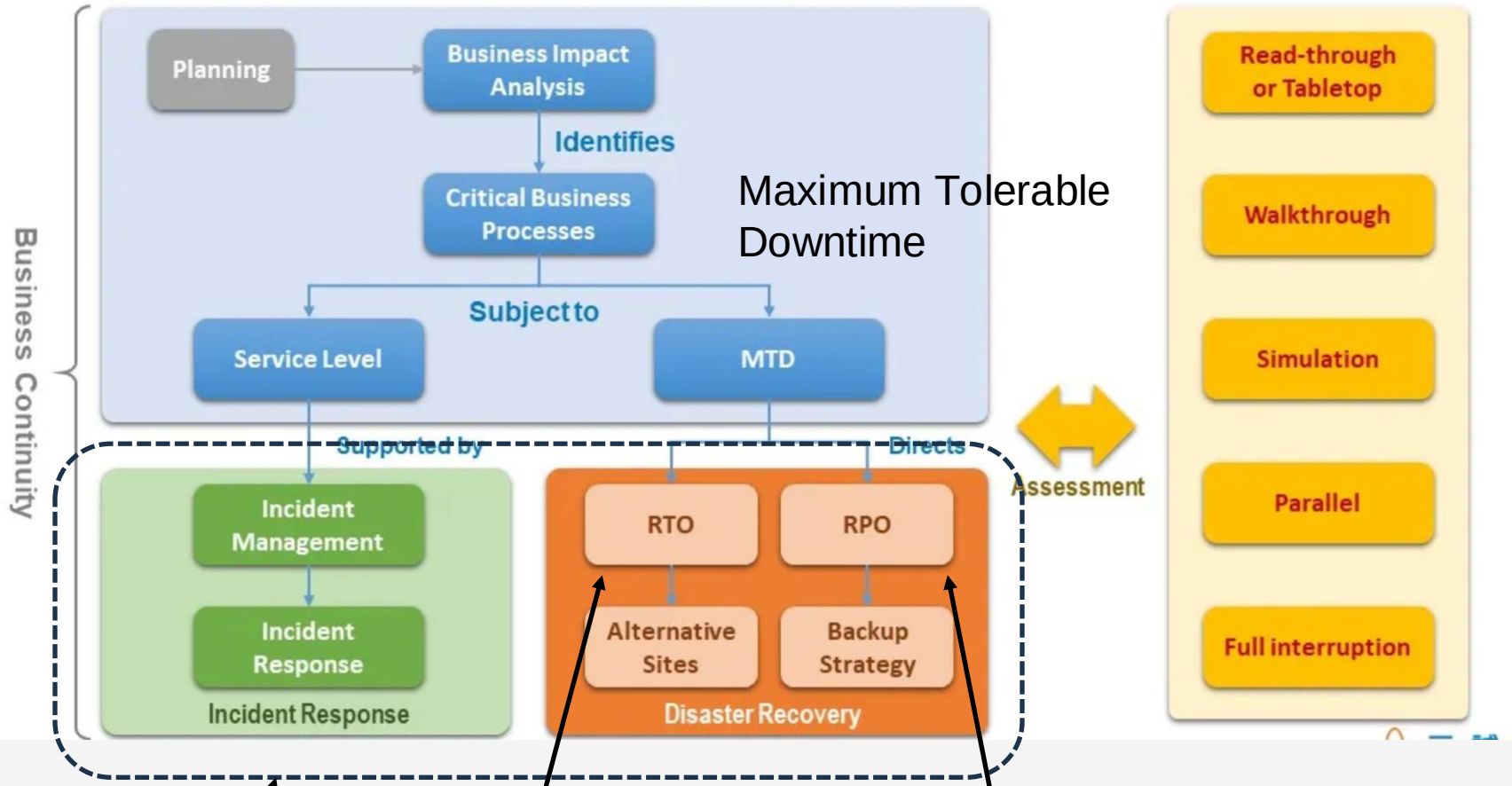
Which interfaces to IS do you see?



Source: https://www.invensislearning.com/blog/risk-management-process-steps/ , https://iso-docs.com/blogs/iso-22301-standard/iso-22301-clause-1-scope , https://www.wallstreetmojo.com/business-continuity-planning/

Business Continuity Management

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Maximum Tolerable Downtime

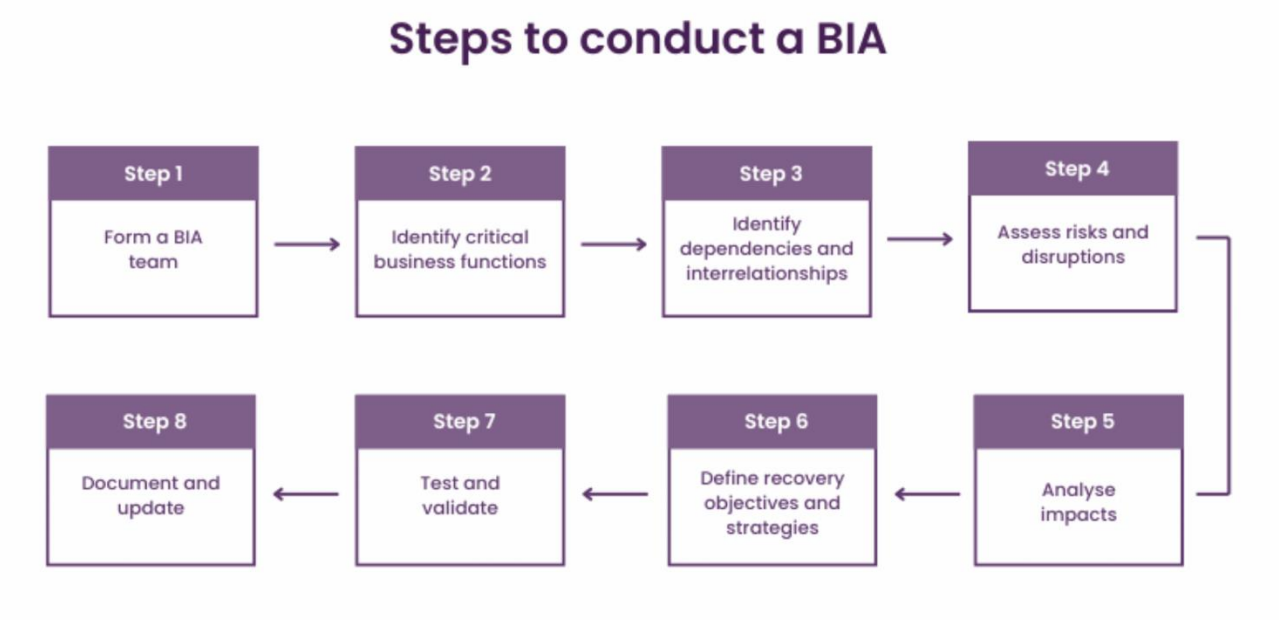
Intersections with IS

Recovery Time Objective
(RTO is the maximum acceptable amount of time that a business process or system can be down after a disaster or disruption before causing significant damage to the business)

Recovery Point Objective
(RPO is the maximum acceptable amount of data loss measured in time. It represents the point in time to which data must be restored following a disaster to resume acceptable normal operations)

In these contexts, Business Impact Analyses are being used

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



	IMPACTS			
	Compliance & Regulatory	Reputation	Financial	Mission
Human Resources	Low	High	Low	High
Information Technology	Low	High	High	High
Product Development	Low	High	High	High
Information Security	High	High	Low	Low
Finance	High	High	Low	High

Source: https://bryghtpath.com/what-is-a-business-impact-analysis-bia/ , https://www.theknowledgeacademy.com/blog/business-impact-analysis/

Case Study

You can also use your own company as case study

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

TechWave Solutions is a mid-sized IT services and consulting company based in London, specializing in cloud computing, cybersecurity, and software development. With a workforce of 500 employees, TechWave serves clients across various sectors, including finance, healthcare, and retail. The company's reputation is built on delivering high-quality, secure, and reliable IT solutions.

Scenario: TechWave Solutions is preparing for an upcoming merger with a larger multinational IT corporation. As part of the due diligence process, the company needs to exercise and strengthen its risk management, business continuity management (BCM), business impact analysis (BIA), and information security management practices.

Key Business Elements:

1. **Primary Services:** Cloud computing, cybersecurity, software development.
2. **Key Resources:** IT infrastructure, proprietary software, client data, skilled workforce.
3. **Critical Departments:** IT, Cybersecurity, Software Development, HR, Finance, and Client Support.

Task: Gather together in groups, and, from this high level description, try to

- Risk Management Plan: Establish some key risks: simulate a small risk identification: Identify risks, assess risks, risk treatment strategies; deliverables: Risk Matrix, Risk Register
- BCM plan: identify critical business functions, assess the impact of their disruption, determine Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), develop continuity strategies (how to maintain operations during various disruption scenarios, including remote work capabilities and data recovery plans), incident response plan
- Try also to discuss the interplay between Risk Management, BCM, IS departments and processes

Case Study - Examples for what to consider

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Cybersecurity Breaches
- IS breaches – externally and internally originated
- System Downtime
- Merger Challenges
- Pandemic / Natural Desaster
- Software Development risks

- There is no right or wrong
- Try to be creative

Question

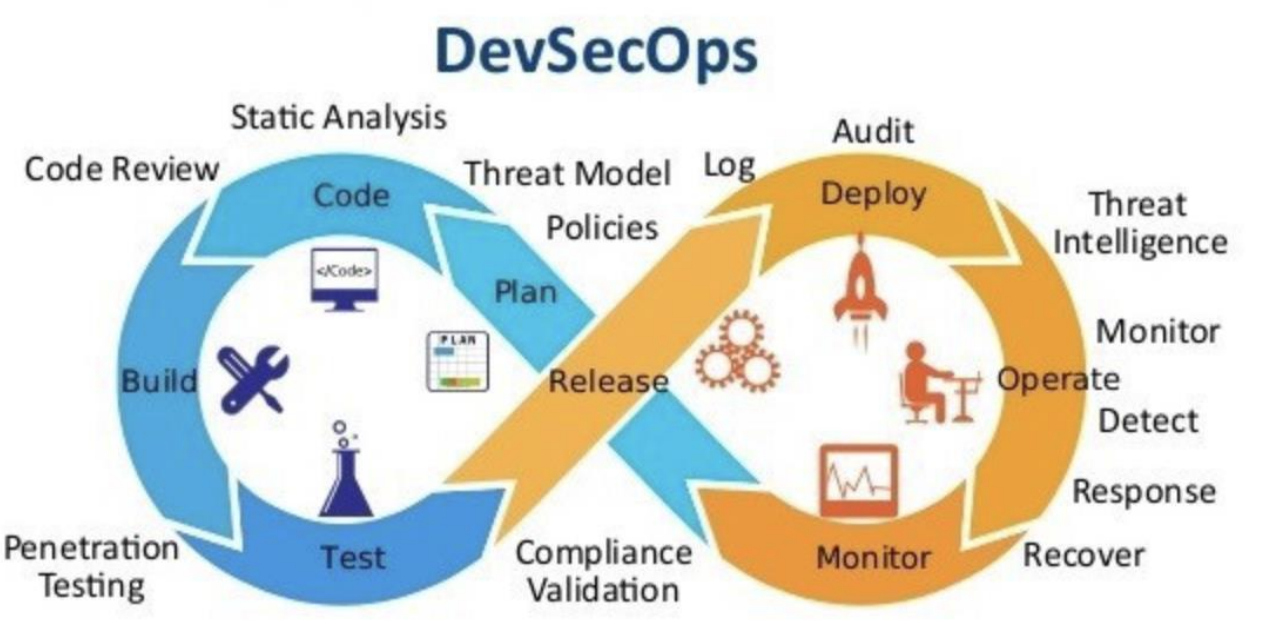
So far, we focussed mostly on detection and response (SOC topics) and Security Strategy.
What other aspects may be of relevance?

Product / Application Security

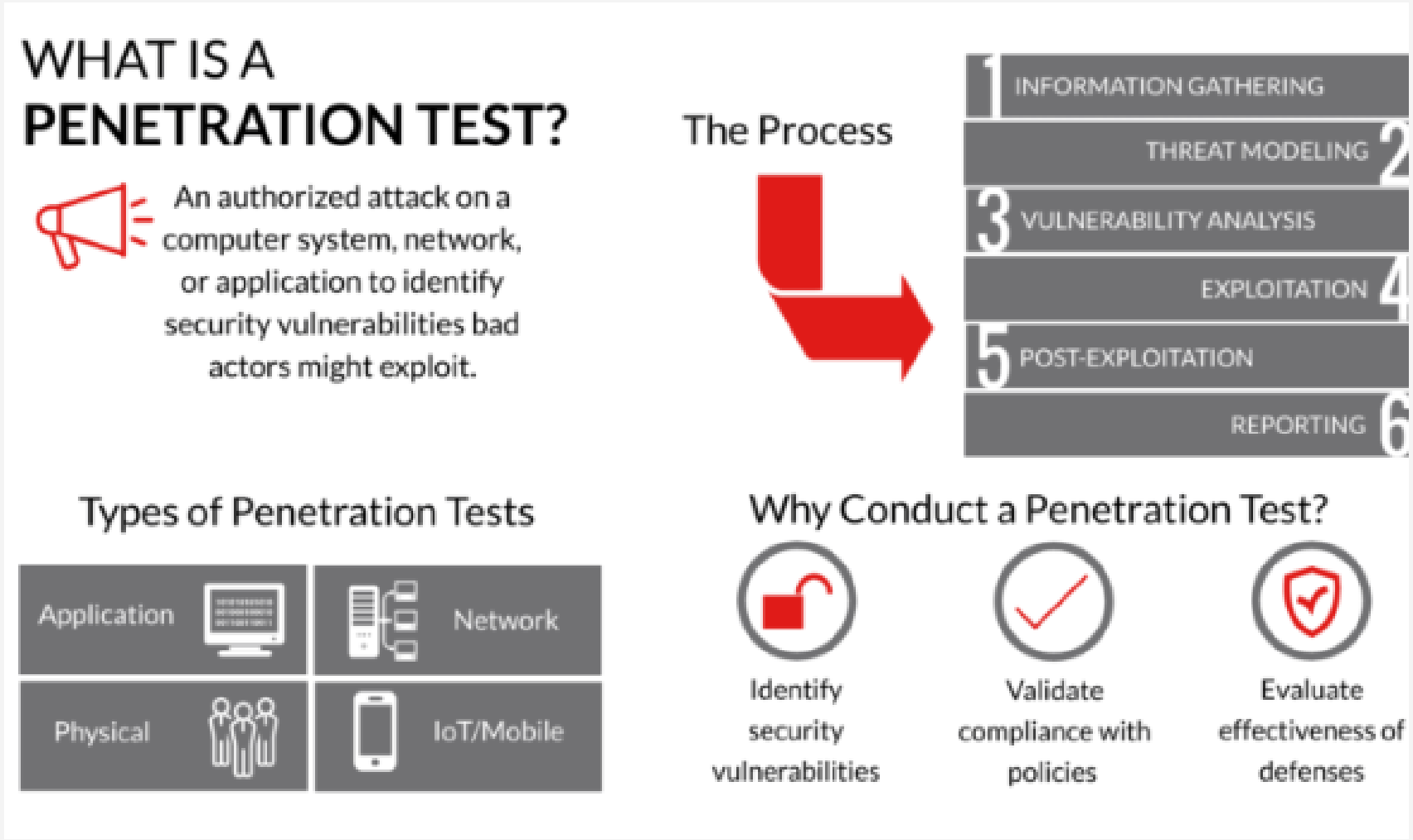
- Idea: Add the security mindset in software development
- While SOC focusses on ”stopping the bleeding” and enhancing the security posture of the company’s assets in general, Product Security focusses on desinging secure products
- Examples of activities:
  - Production Readiness Reviews
  - Architectural reviews
  - Developing secure solutions to mitigate risks
- → More on that when we get to Security Architectures

DevSecOps

- Enrich DevOps by automated checks, processes, tech, e.g. automated static analyses built into the CI/CD pipeline
- shift left for security in the development lifecycle



Offensive Security



Source: https://plextrac.com/blog/what-is-a-penetration-test/

Question

What kind of skills do you consider relevant for the various security positions?

- SOC
- IAM
- Product / Application Security
- CISO
- Security Engineering
- Compliance / ISMS
- …

Question

What may be the purpose, the idea behind introducing an IS framework?

Why use Security Frameworks?

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Provide a structured approach to managing information security
- Help organizations comply with regulations and standards
- Facilitate risk management and incident response
- Enhance customer and stakeholder confidence

Overview of ISO 27001

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- International Standard for Information Security Management Systems (ISMS)
- Focuses on a risk management process to secure information assets

Key Components

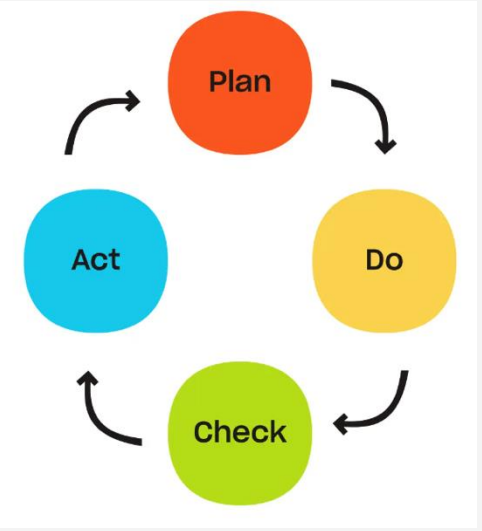
- **ISMS Scope:** Define the boundaries and context of the ISMS
- **Risk Assessment:** Identify and evaluate information security risks
- **Controls:** Implement controls to mitigate identified risks
- **Continuous Improvement:** Regularly review and update the ISMS

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

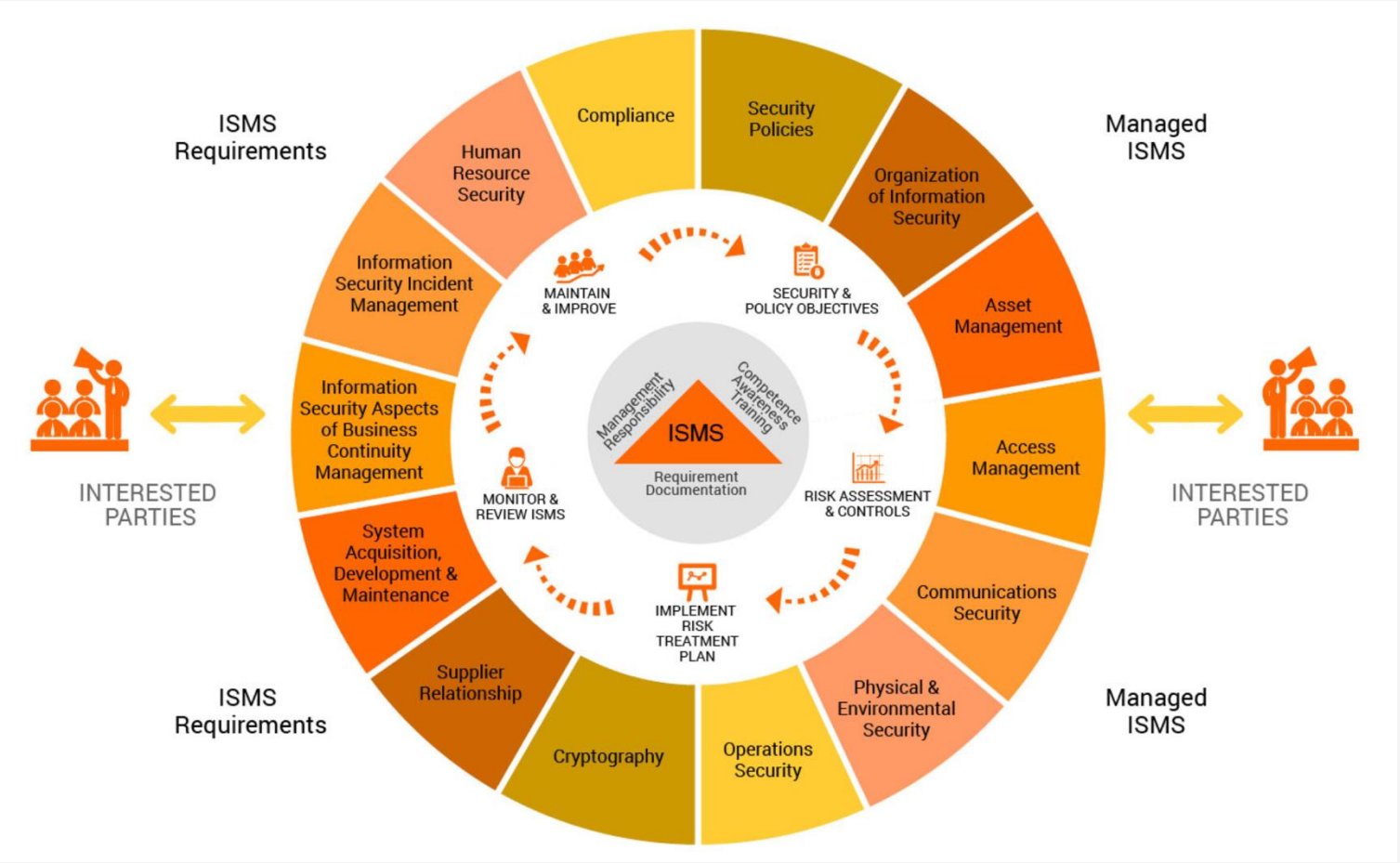
What is an ISMS?

An Information Security Management System (ISMS) is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives.

It encompasses people, processes, and IT systems by applying a risk management process to daily data management workflows.



ISMS Overview



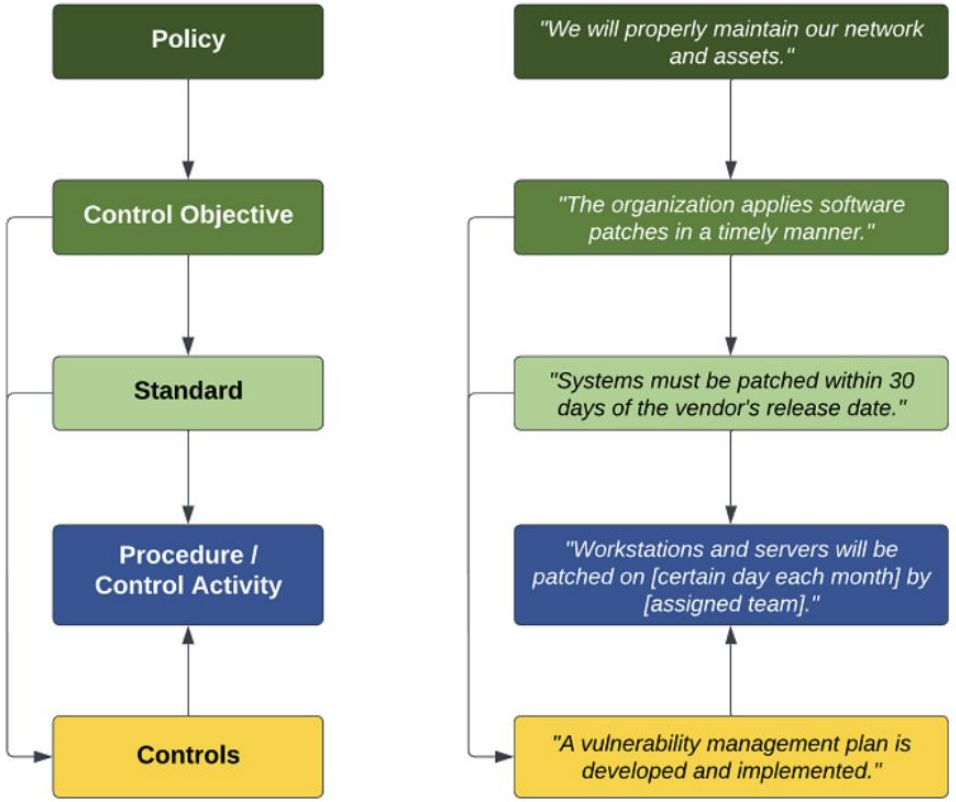
Source: https://ccqm.ch/certification-process/iso-iec-27001-information-security-management-system/

Key Domains in ISO 27001

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Hierarchy of Documents in a Company's IS framework

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



DESCRIPTION

Policies are "high level" statements of management's intent and are intended to guide decisions to achieve rational outcomes. Policies are not meant to be prescriptive, but provide an overall direction for the organization.

Control Objectives support policy by identifying applicable requirements that the organization needs to address. These applicable requirements can be best practices, laws or other legal obligations.

Standards establish formal requirements in regards to processes, actions and configurations. Standards are entirely focused on providing narrowly-focused, prescriptive requirements that are quantifiable.

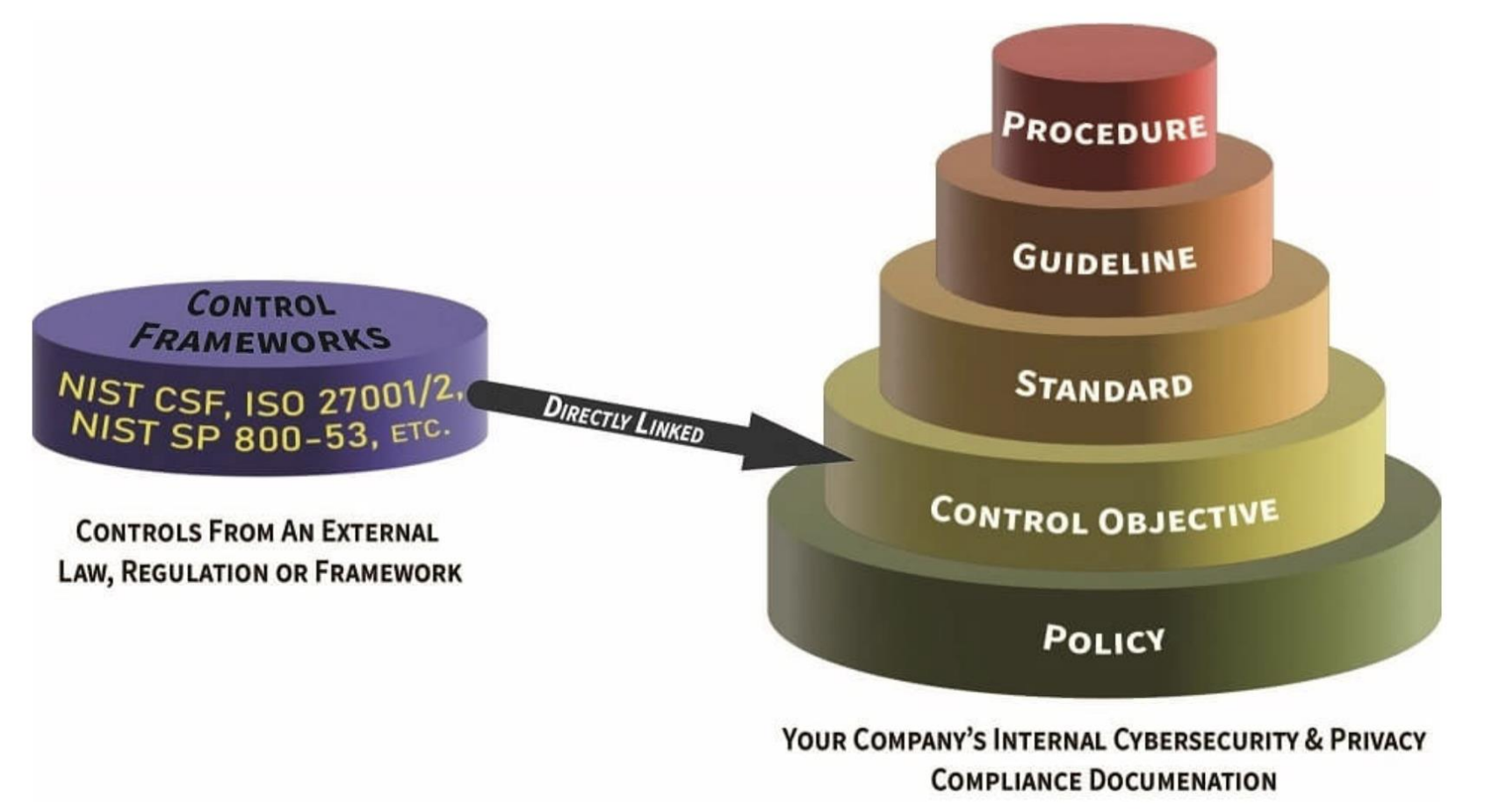
Procedures are formal methods of performing a task, based on a series of actions conducted in a defined and repeatable manner.

Controls are technical or administrative safeguards that may prevent, detect or lessen the ability of the threat actor to exploit a vulnerability.

Source: https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-procedure

Hierarchy of Documents in a Company's IS framework

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

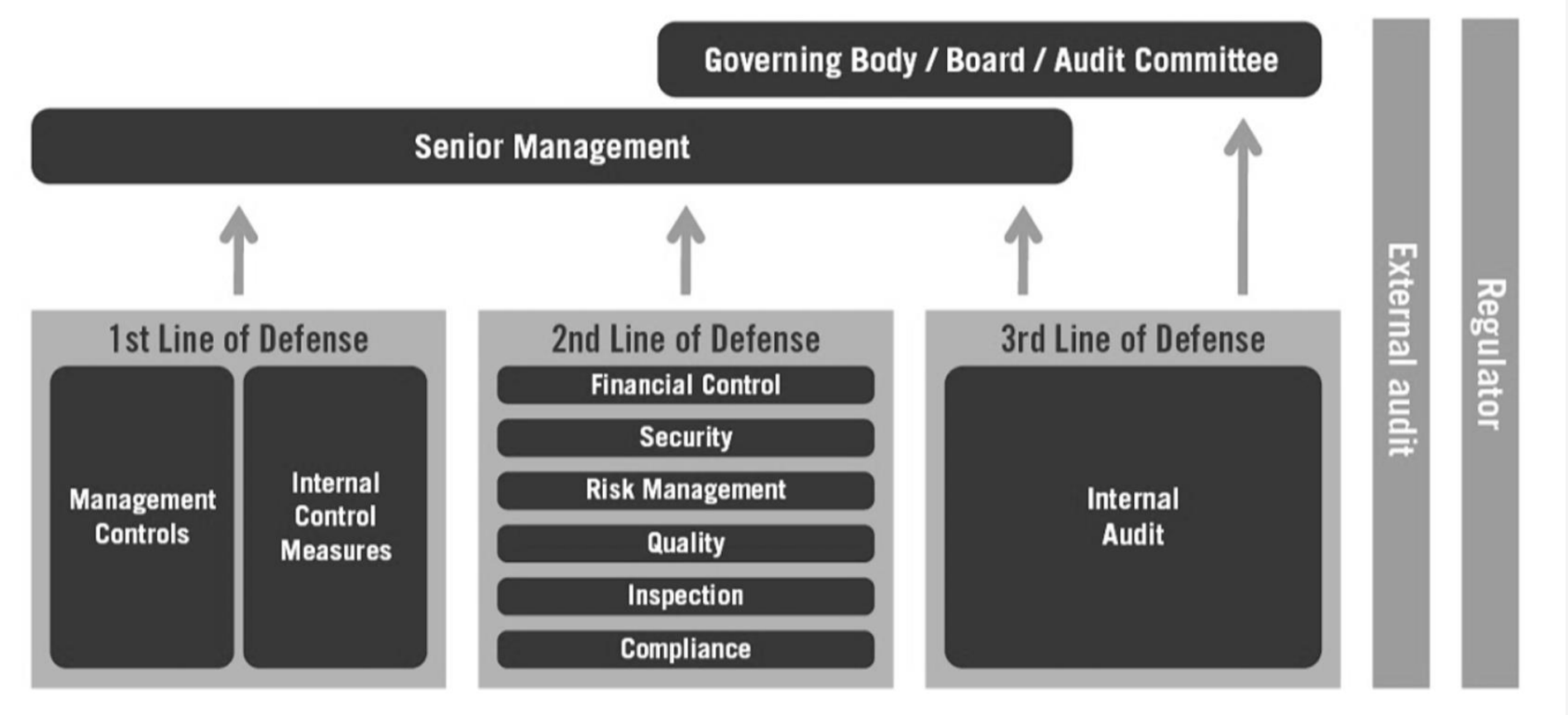


Source: https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-procedure

Towards setting up ISO 27001

- InfoSec Policy (high level principles, responsibilities etc.)
- Control Objectives and Controls (Risk Assessment → select appropriate controls)
- Risk Management Policy (How risks are identified, assessed etc.)
- Access Control Policy
- Asset Management Policy
- Crypto Policy
- Physical and Environmental Security Policy
- Communications and Operations Management Policy
- Incident Management Policy
- Supplier Relationships Policy
- Business Continuity Policy
- Compliance Policy (regulatory requirements)
- HR Policy

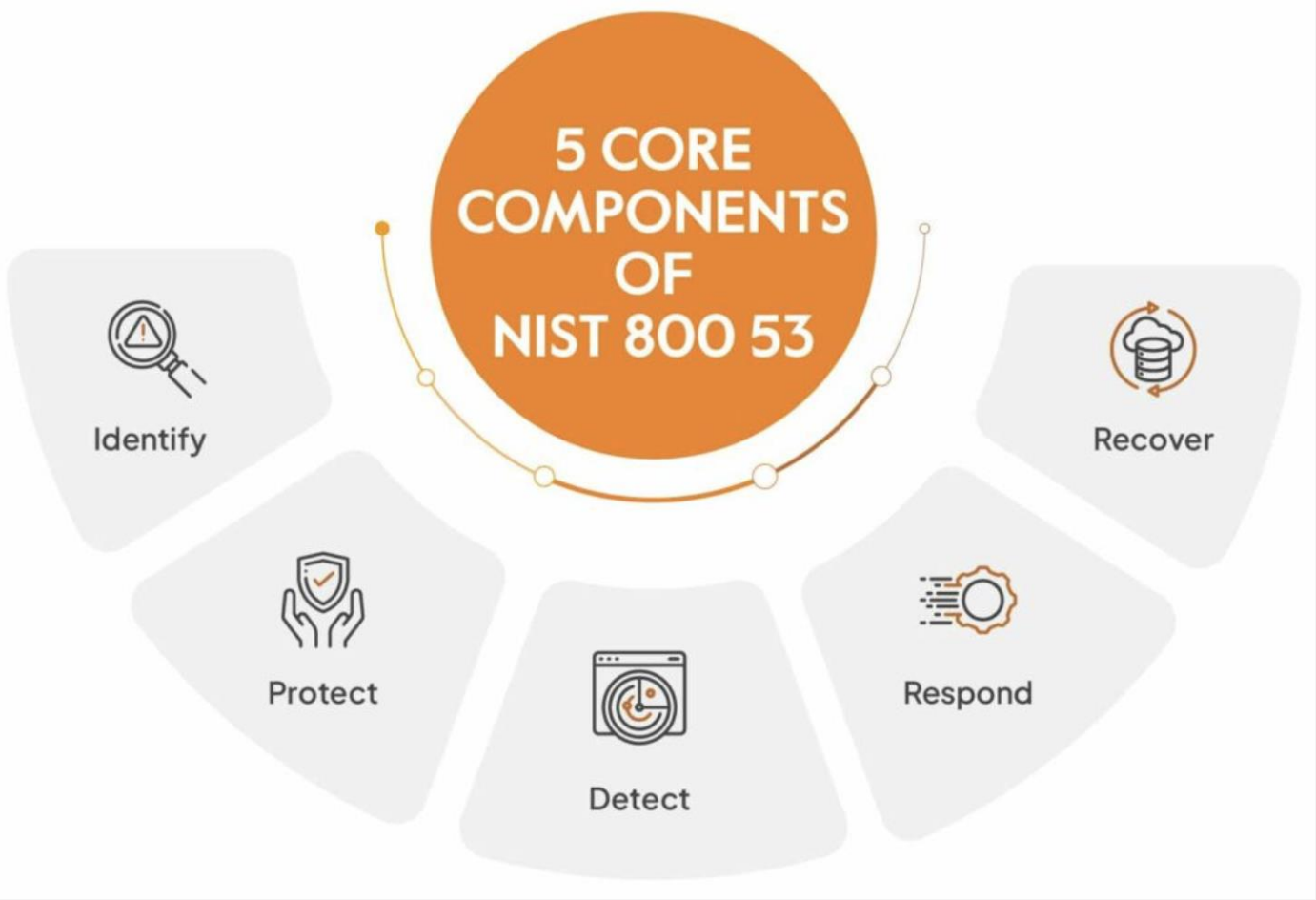
Three Lines of Defense Approach



Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

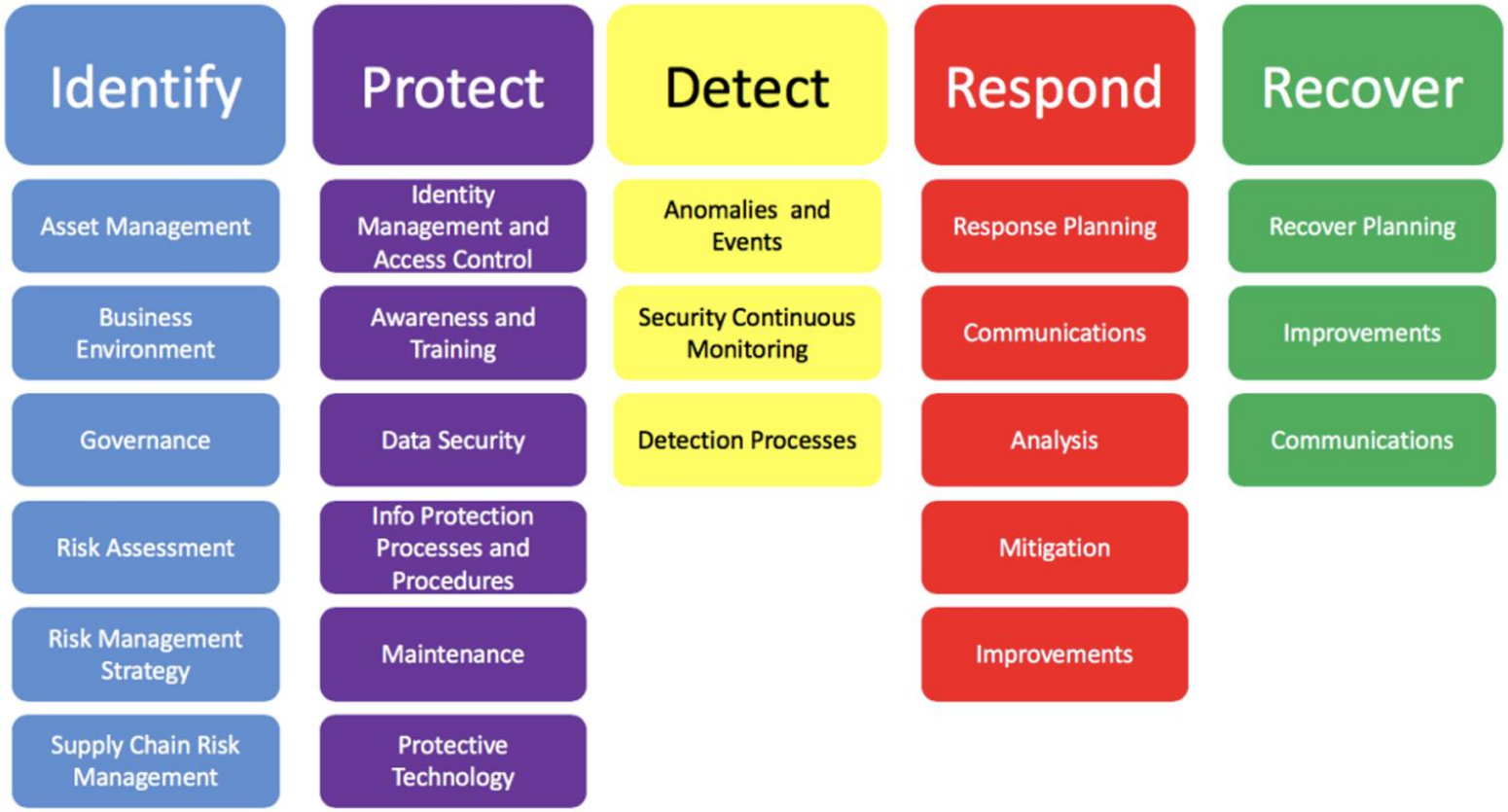
NIST Cybersecurity Framework

- Framework that provides structure to manage cybersecurity risks
- Core consists of 5 concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover
- Four Tiers for a maturity level: Partial, Risk Informed, Repeatable, Adaptive
- Tailoring: according to organization's business requirements, risk appetite, resources, environment etc.



Source: https://sprinto.com/blog/nist-800-53-guide/

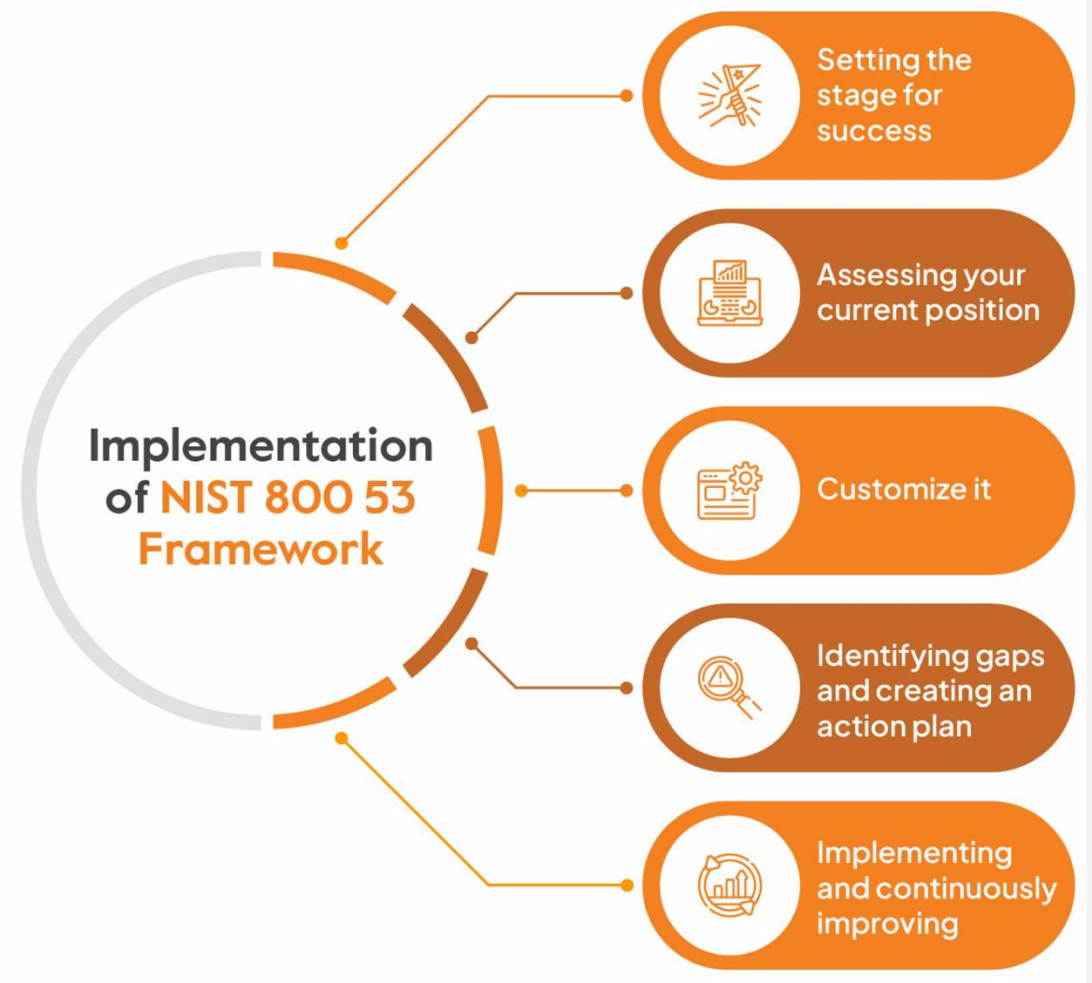
NIST Cybersecurity Framework



Source: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018

Implementing NIST

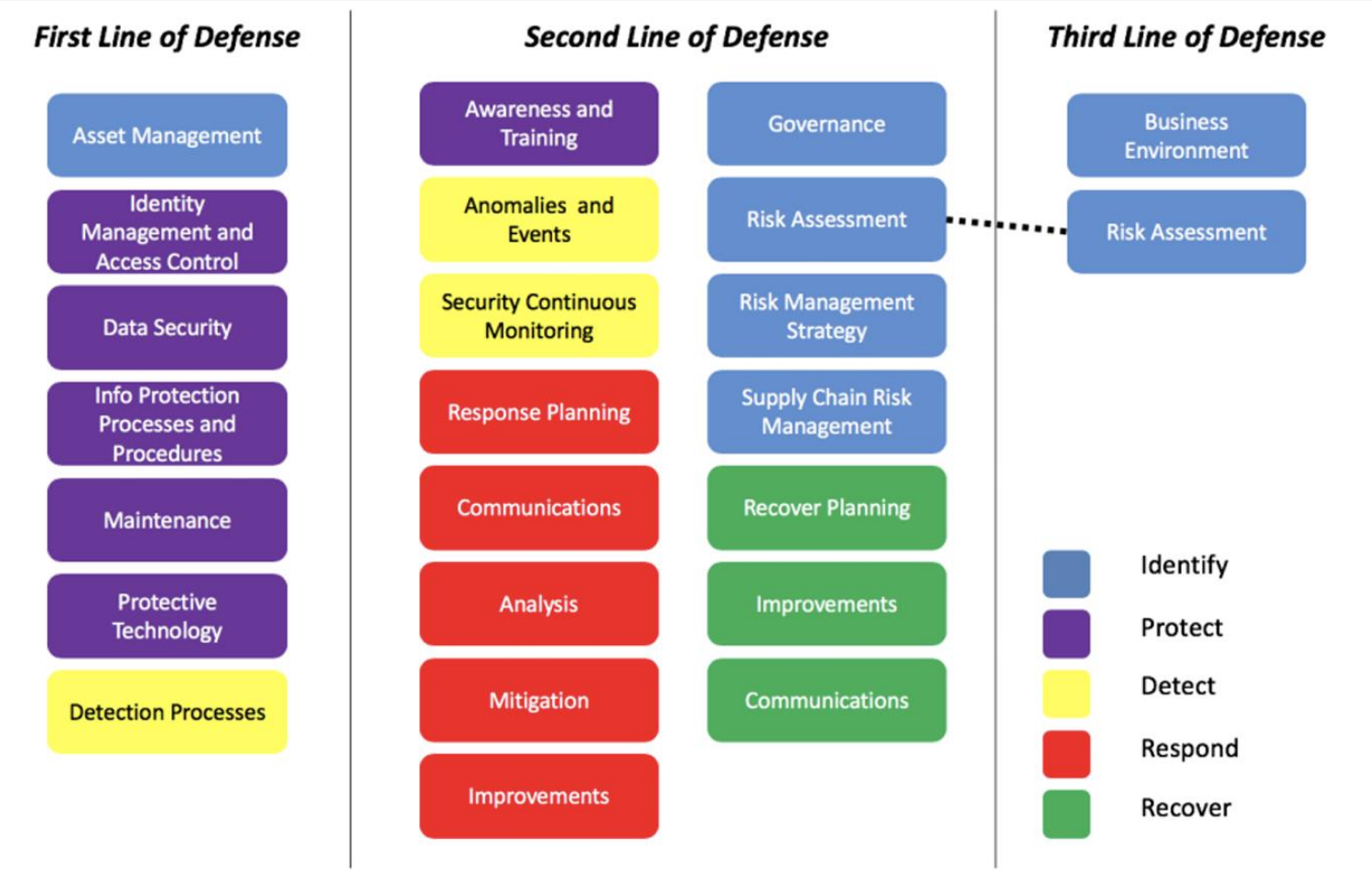
- NIST also follows a PDCA cycle
- After typical assessment of the current situation and tailoring to the own organization, executing the plan, thereby reducing the gap between status quo and desired goal, a continuous improvement cycle begins



Source: https://sprinto.com/blog/nist-800-53-guide/

Mapping Cybersecurity Framework to Three Lines of Defense

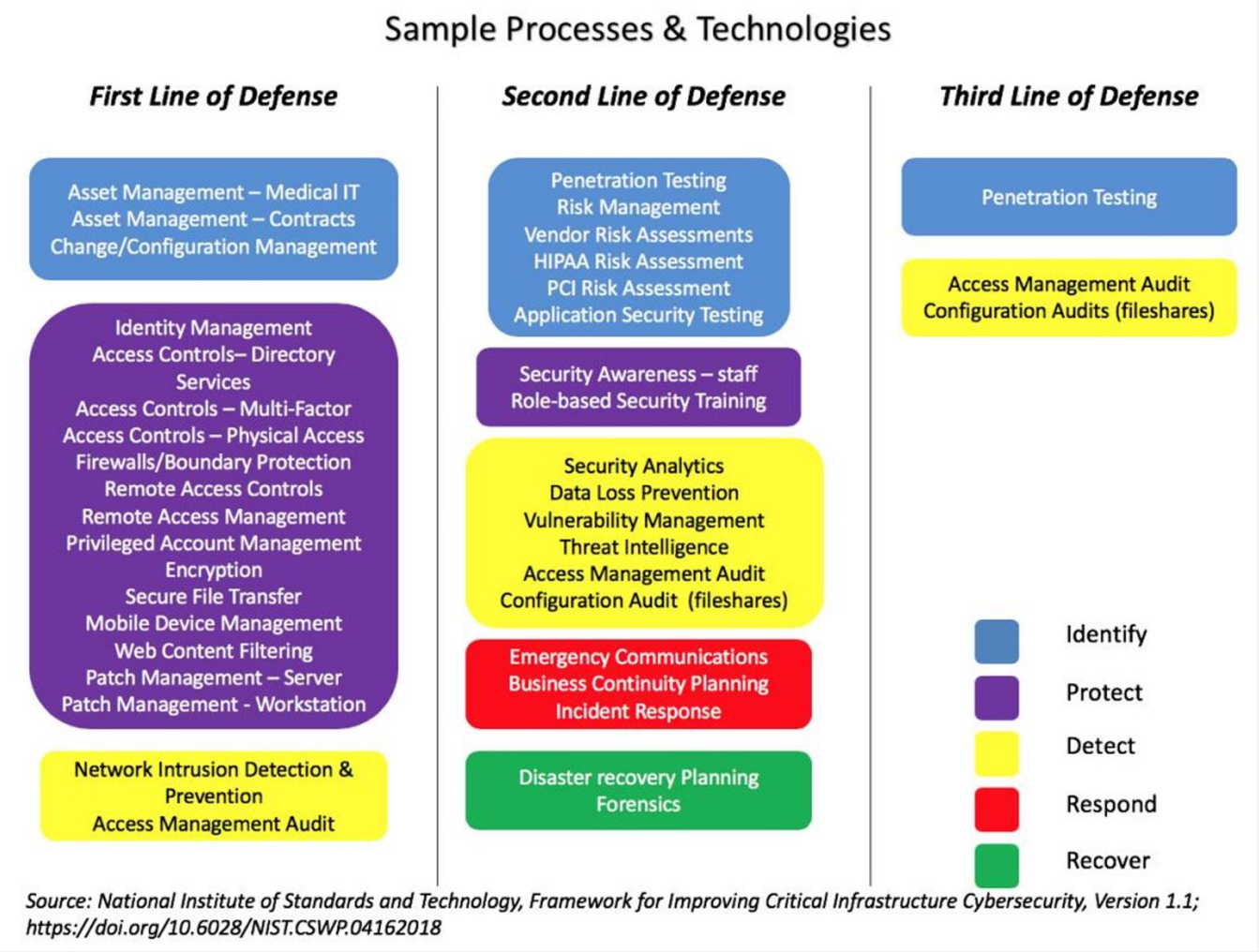
Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Source: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018

Sample Processes and Technology Mapping

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Source: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018

NIST SP 800-53

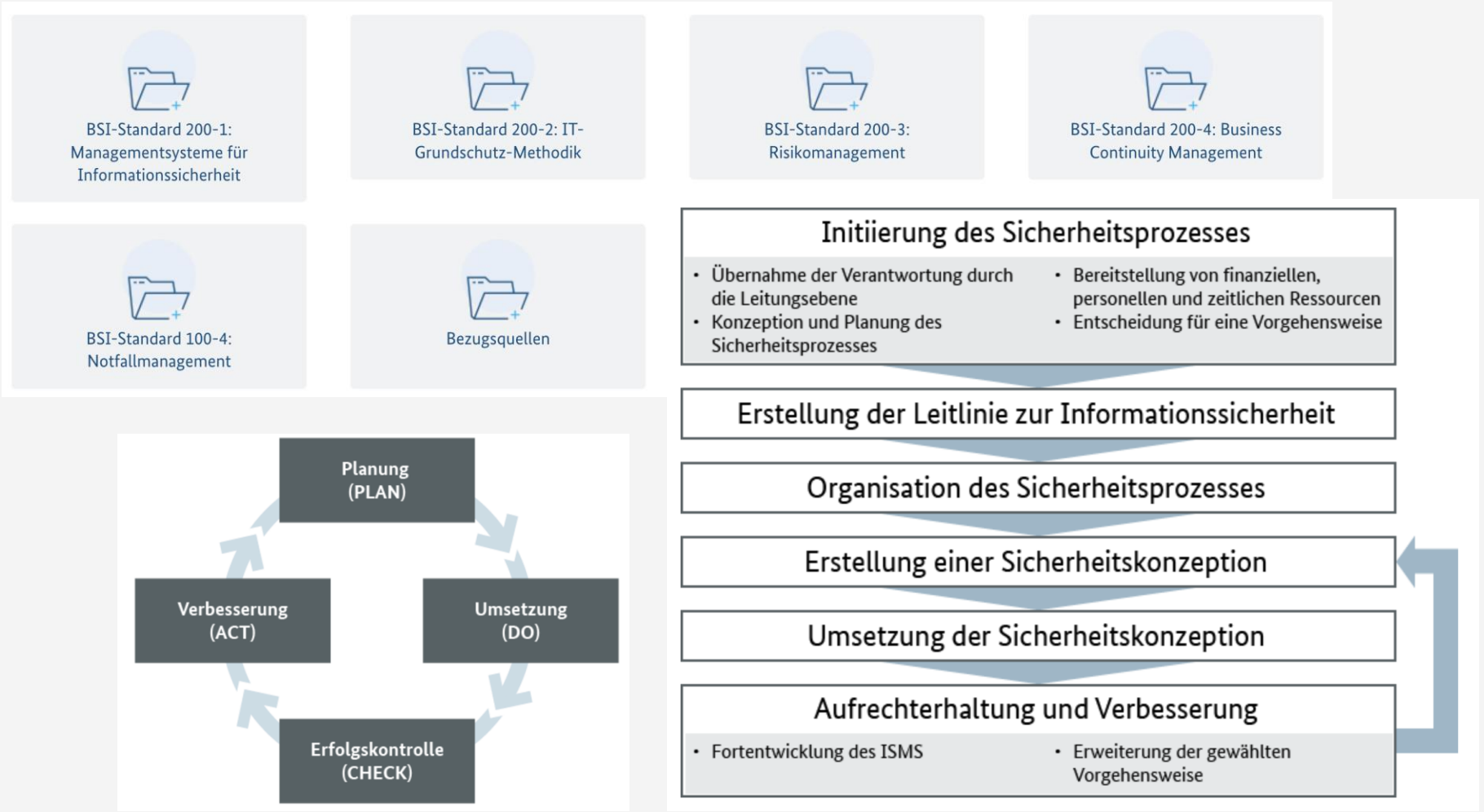
- “Security and Privacy Controls for Information Systems and Organizations”
- Catalog of controls (security and privacy)
- Split into 18 control families
- Controls split into three impact levels (low, moderate, high)
- Privacy controls as well

Control Families

AC	ACCESS CONTROL
AT	AWARENESS AND TRAINING
AU	AUDIT AND ACCOUNTABILITY
CA	ASSESSMENT, AUTHORIZATION, AND MONITORING
CM	CONFIGURATION MANAGEMENT
CP	CONTINGENCY PLANNING
IA	IDENTIFICATION AND AUTHENTICATION
IR	INCIDENT RESPONSE
MA	MAINTENANCE
MP	MEDIA PROTECTION
PE	PHYSICAL AND ENVIRONMENTAL PROTECTION
PL	PLANNING
PM	PROGRAM MANAGEMENT
PS	PERSONNEL SECURITY
PT	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY
RA	RISK ASSESSMENT
SA	SYSTEM AND SERVICES ACQUISITION
SC	SYSTEM AND COMMUNICATIONS PROTECTION
SI	SYSTEM AND INFORMATION INTEGRITY
SR	SUPPLY CHAIN RISK MANAGEMENT

BSI Grundschutz

- Framework from Bundesamt für Sicherheit in der Informationstechnik (BSI)
- IT-Grundschutz-Kompendium: central document with controls
- Sicherheitsprozess: continuous process to manage information security



Source: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/

Task: Another approach – OWASP ASVS

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Make yourself familiar with OWASP ASVS and present its main characteristics

A task for one group

Task: Compare the approaches yourself

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Compare ISO 27001, NIST framework, NIST SP 800-53, BSI Grundschutz and draw your conclusions

A task for one group

Task: Presentations about your Security Organization

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Gather in groups with relative homgenity from a company affiliation perspective
- Each group: Prepare a brief presentation (15-20 minutes) that gives an overview on the IS organization in your company
- Aspects:
  - Organizational Setup
  - Selection of Processes & Tools
  - If you are part of InfoSec – where and how do you work there – if not, how do you interact with InfoSec
  - Selection of interesting aspects (e.g. example of an incident response, code review)
  - Also consider BCM, Risk Management etc.
- Presentations next week (one after another)

Task for multiple groups (multiple companies)