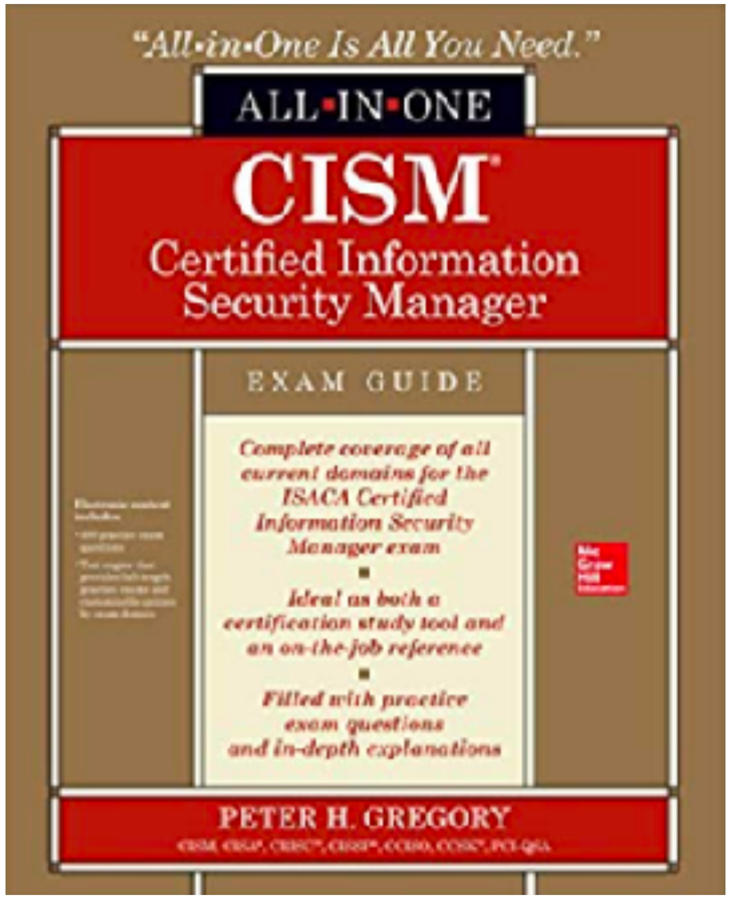
CNIT 160: Cybersecurity Responsibilities

2. Information Security Governance

Part 1

Pages 16 - 55


"All-in-One Is All You Need."
ALL▪IN▪ONE
CISM
Certified Information Security Manager
EXAM GUIDE
Complete coverage of all current domains for the ISACA Certified Information Security Manager exam
Ideal as both a certification study tool and an on-the-job reference
Filled with practice exam questions and in-depth explanations
PETER H. GREGORY

Topics in Part 1

- **Introduction to Information Security Governance**
  - **Reason for Security Governance**
  - **Security Governance Activities and Results**
  - **Business Alignment**
  - **Roles and Responsibilities**

Topics in Part 1 (continued)

- **Introduction to Information Security Governance (continued)**
  - **Monitoring Responsibilities**
  - **Information Security Governance Metrics**
  - **The Security Balanced Scorecard**
  - **Business Model for Information Security**

Topics in Part 2

- **Security Strategy Development**
  - **Strategy Objectives**
  - **Control Frameworks**
  - **Risk Objectives**
  - **Strategy Resources**
  - **Strategy Development**
  - **Strategy Constraints**

Governance

- **A process whereby senior management exerts strategic control over business functions**
- **Through policies, objectives, delegation of authority, and monitoring**
- **Ensures that business processes effectively meet vision and objectives**

Information Security Governance

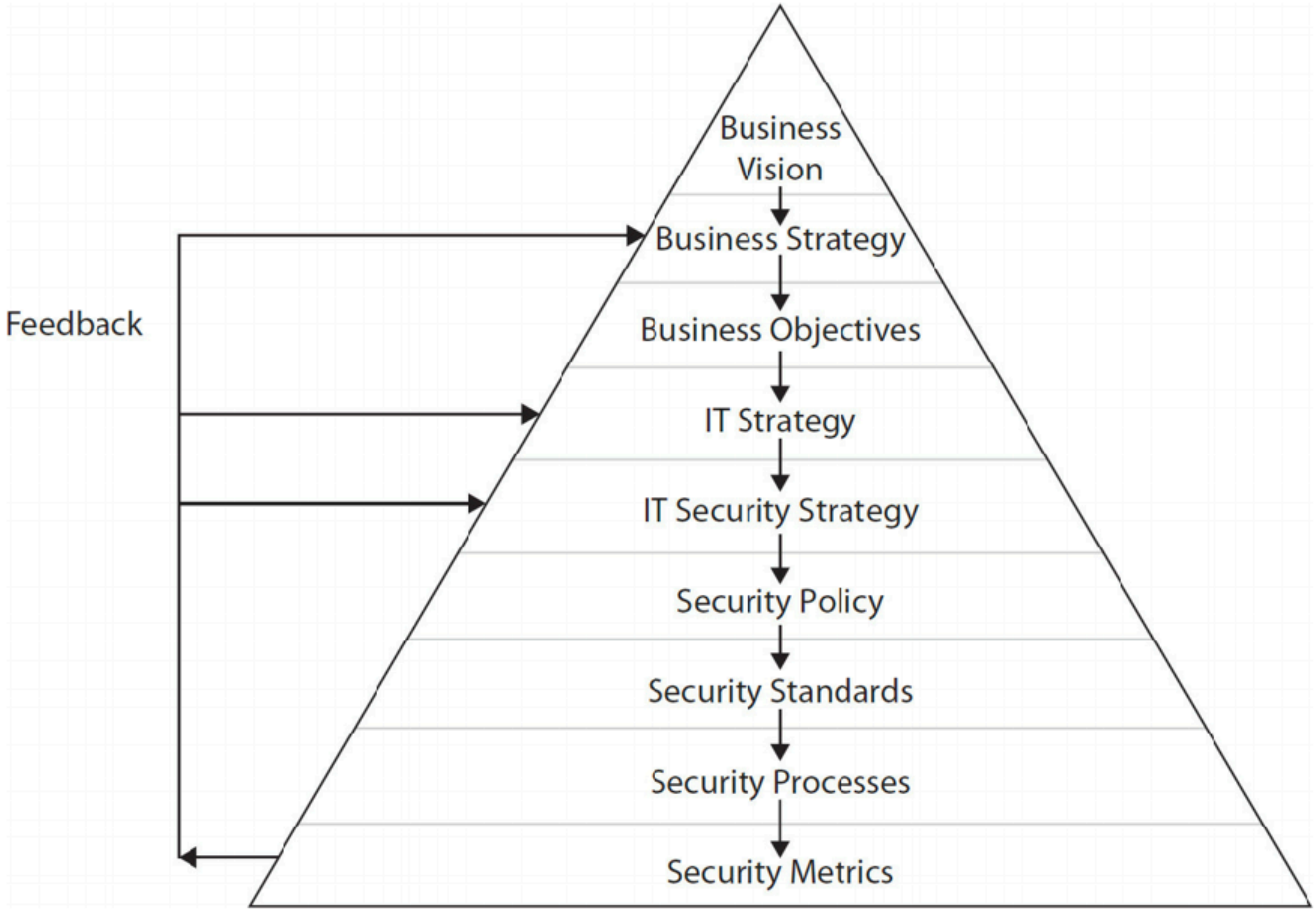
- **Focuses on key processes**
    - **Personnel management**
    - **Sourcing**
    - **Risk management**
    - **Configuration management**
    - **Change management**
    - **Access management**

Information Security Governance

- Focuses on key processes (continued)
  - Vulnerability management
  - Incident management
  - Business continuity planning
- Establishment of an effective organization structure and clear statements of roles and responsibilities

Information Security Governance

- ***Monitor*** **processes with scorecard or metrics**
- ***Continuous improvement*** **changes processes to keep them effective and support ongoing business needs**


Business Vision
Business Strategy
Business Objectives
IT Strategy
IT Security Strategy
Security Policy
Security Standards
Security Processes
Security Metrics
Feedback

- **Objectives** These are desired capabilities or end states, ideally expressed in achievable, measurable terms.
- **Strategy** This is a plan to achieve one or more objectives.
- **Policy** At its minimum, security policy should directly reflect the mission, objectives, and goals of the overall organization.
- **Priorities** The priorities in the security program should flow directly from the organization's mission, objectives, and goals. Whatever is most important to the organization as a whole should be important to information security as well.

- **Standards** The technologies, protocols, and practices used by IT should be a reflection of the organization's needs. On their own, standards help to drive a consistent approach to solving business challenges; the choice of standards should facilitate solutions that meet the organization's needs in a costeffective and secure manner.
- **Processes** These are formalized descriptions of repeated business activities that include instructions to applicable personnel. Processes include one or more procedures, as well as definitions of business records and other facts that help workers understand how things are supposed to be done.
- **Controls** These are formal descriptions of critical activities to ensure desired outcomes.

- **Program and project management** The organization’s IT and security programs and projects should be organized and performed in a consistent manner that reflects business priorities and supports the business.
- **Metrics/reporting** This includes the formal measurement of processes and controls so that management understands and can measure them.

Reason for Security Governance

- **Organizations are dependent on information systems**
- **Must understand priority of**
  - **Confidentiality**
  - **Integrity**
  - **Availability**

Security Governance Activities and Results

- **Risk management**
  - **Risk assessments and follow-up actions to reduce risks**
- **Process improvement**
- **Event identification**
  - **Security events and incidents**
- **Incident response**

Security Governance Activities and Results

- **Improved compliance**
  - **With laws, regulations, and standards**
- **Business continuity and disaster recovery planning**
- **Metrics management**
  - **Measure key security events, such as incidents, policy changes, violations, audits, and training**

Security Governance Activities and Results

- **Resource management**
  - **Allocation of manpower, budget, and resources**
- **Improved IT governance**
- **Increased trust**
  - **From customers, suppliers and partners**
- **Improved reputation**

Business Alignment

- Security program must align with guiding principles
- Mission
  - Why the organization exists
- Goals and objectives
  - What achievements it wants to accomplish
- Strategy
  - Activities needed to fulfill goals and objectives

Organization's Characteristics

- **Culture**
- **Asset value**
- **Risk tolerance**
- **Legal obligations**
- **Market conditions**

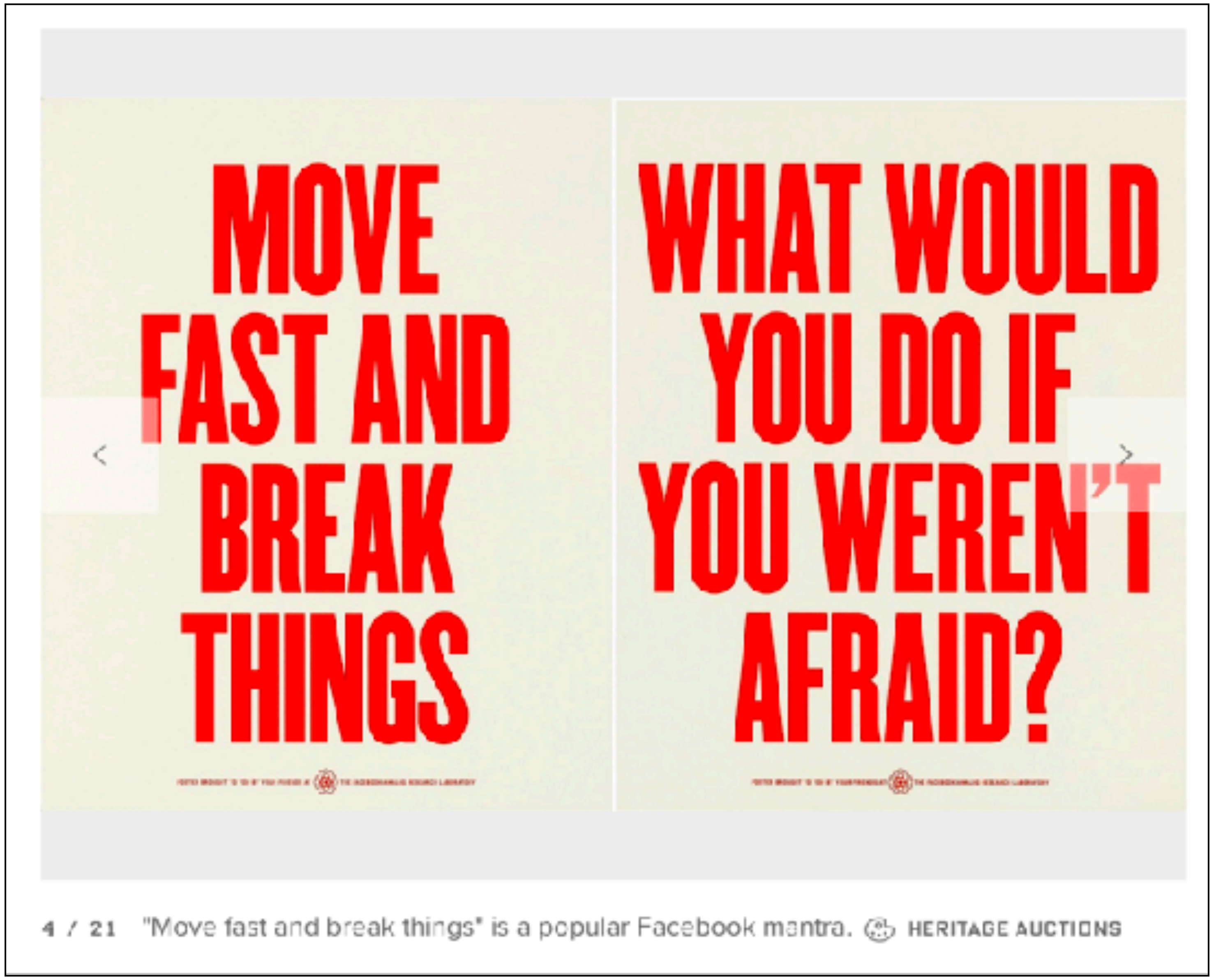
Dr. No

- Security that prevents necessary business practices
- Leads to "Shadow IT"
  - Departments setting up uncontrolled IT assets

Organization's Characteristics

- **Goals and objectives**
- **Risk appetite**
  - **Risk-averse organizations have a formal system of accountability for risk decisions**

Facebook

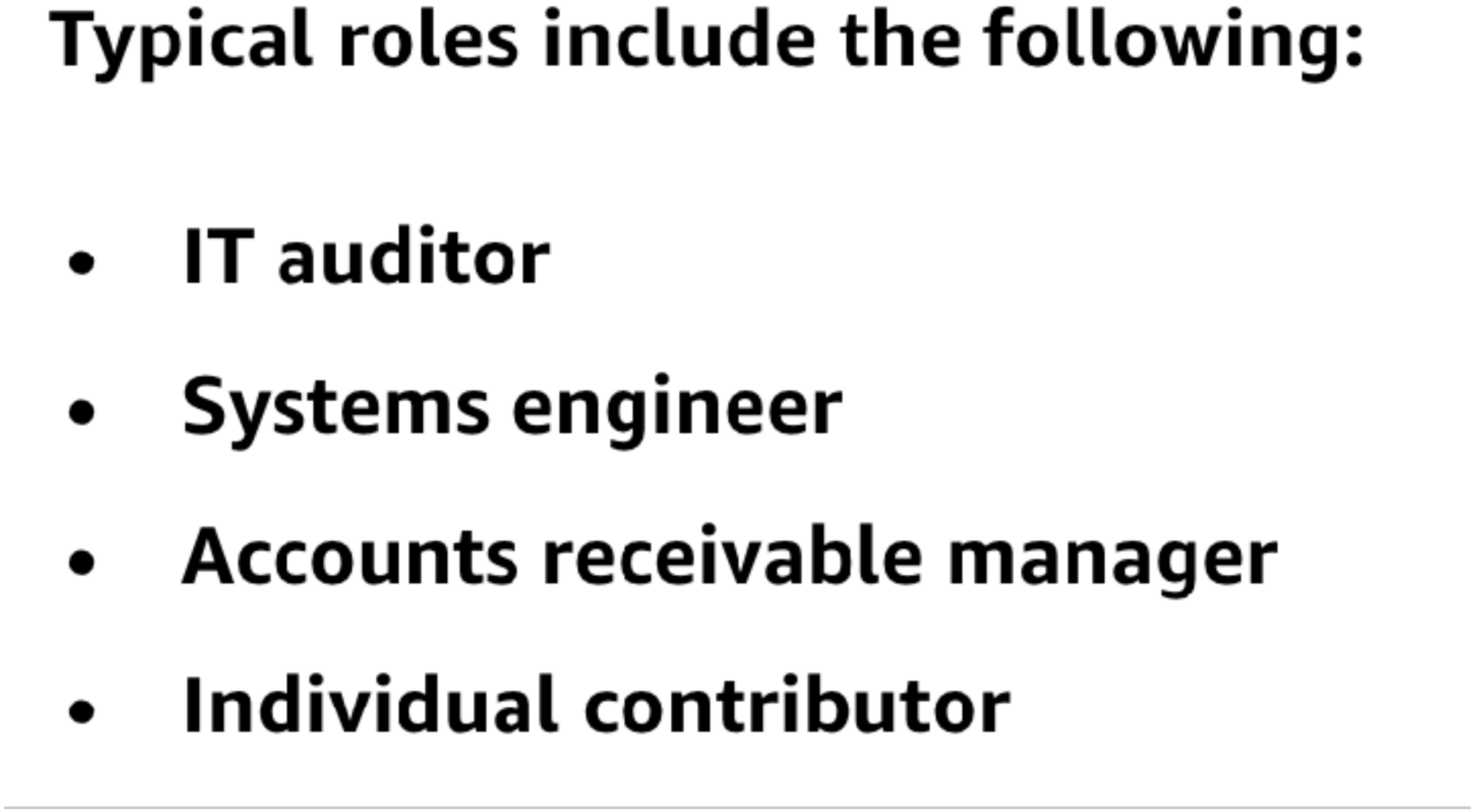

MOVE FAST AND BREAK THINGS
WHAT WOULD YOU DO IF YOU WEREN'T AFRAID?

4 / 21 "Move fast and break things" is a popular Facebook mantra. HERITAGE AUCTIONS

- https://www.wired.com/2016/11/buy-facebook-propaganda-posters/

Roles and Responsibilities

- **Role describes expected activities**

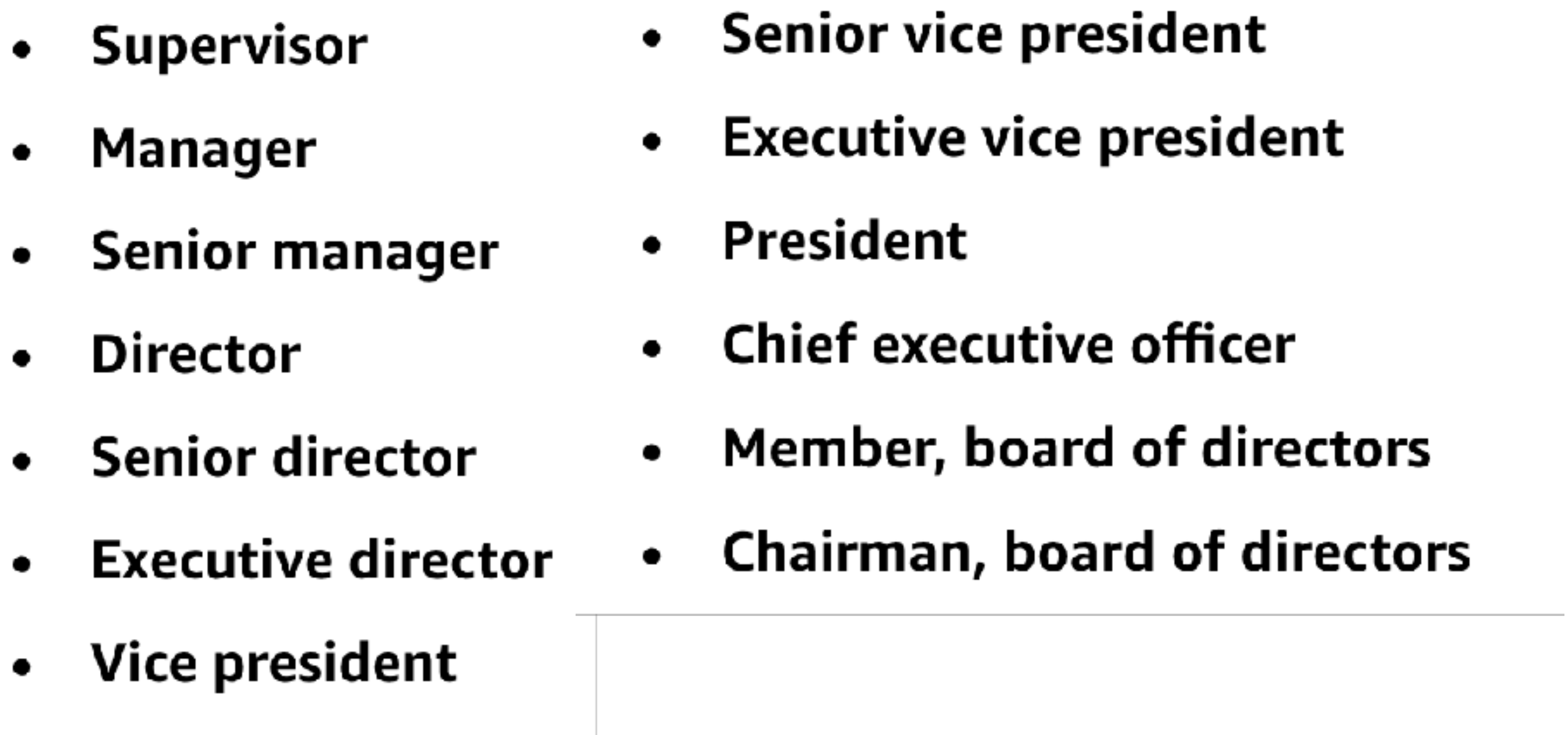


Typical roles include the following:

- **IT auditor**
- **Systems engineer**
- **Accounts receivable manager**
- **Individual contributor**

Ranks

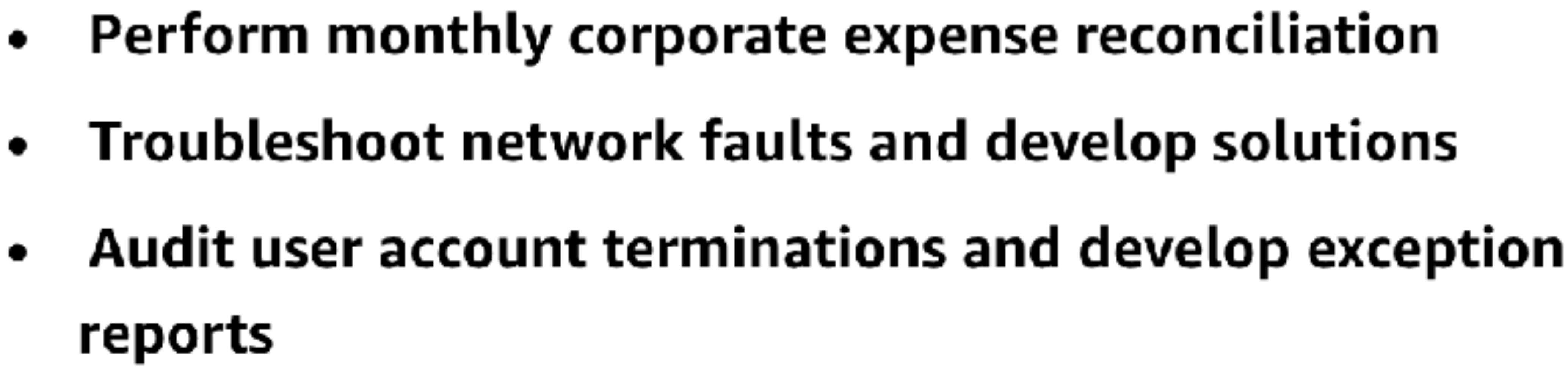
- **In order of increasing seniority**



- Supervisor
- Manager
- Senior manager
- Director
- Senior director
- Executive director
- Vice president
- Senior vice president
- Executive vice president
- President
- Chief executive officer
- Member, board of directors
- Chairman, board of directors

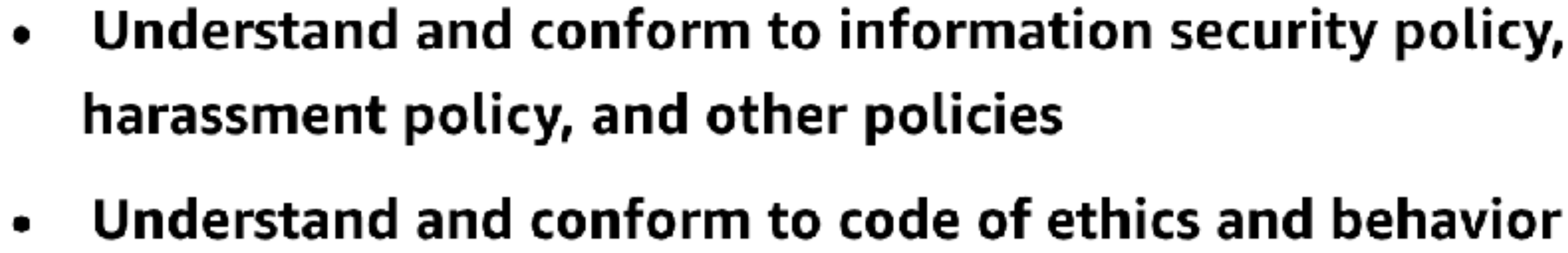
Responsibilities

- **Specific**



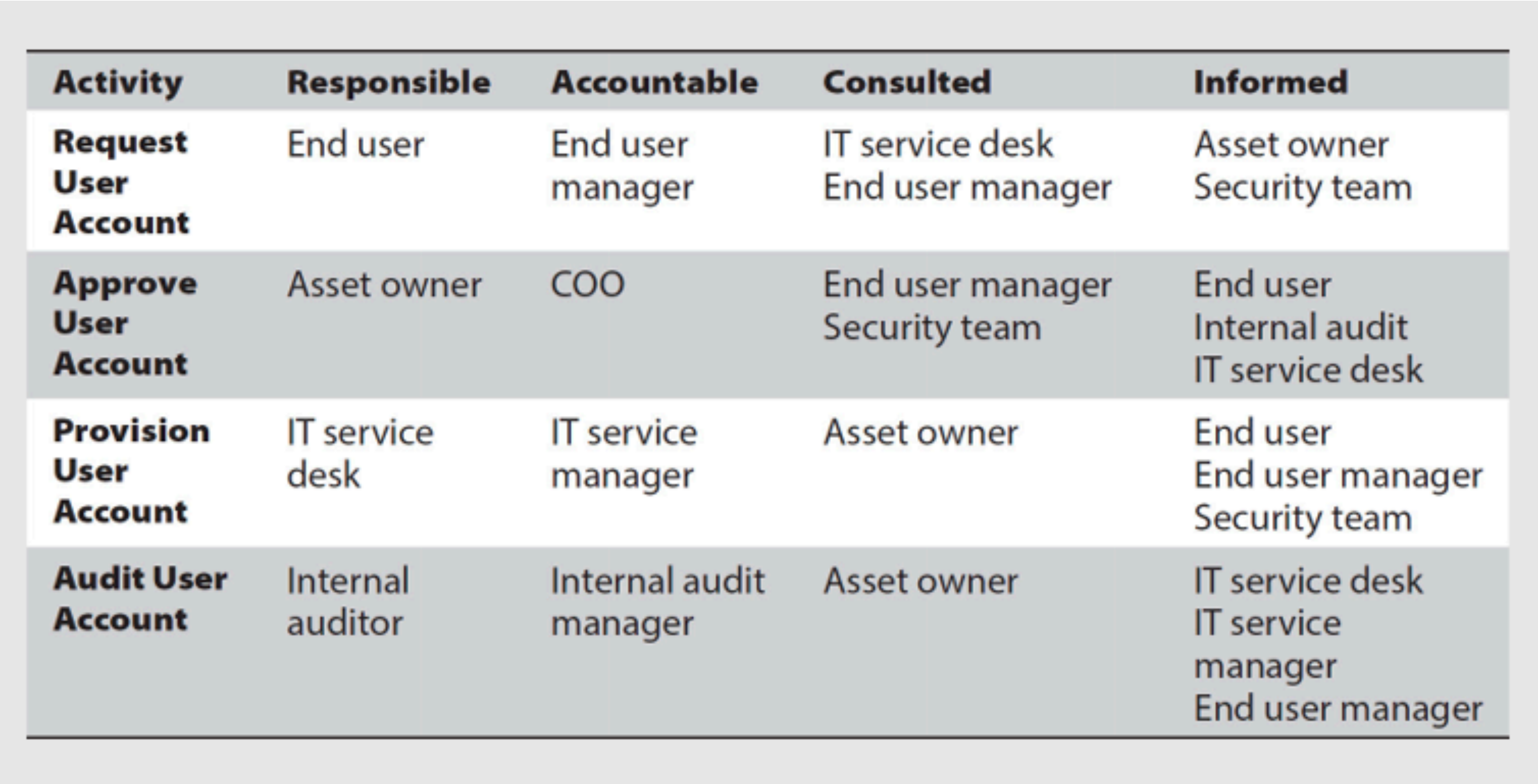
  - **Perform monthly corporate expense reconciliation**
  - **Troubleshoot network faults and develop solutions**
  - **Audit user account terminations and develop exception reports**

- **General**



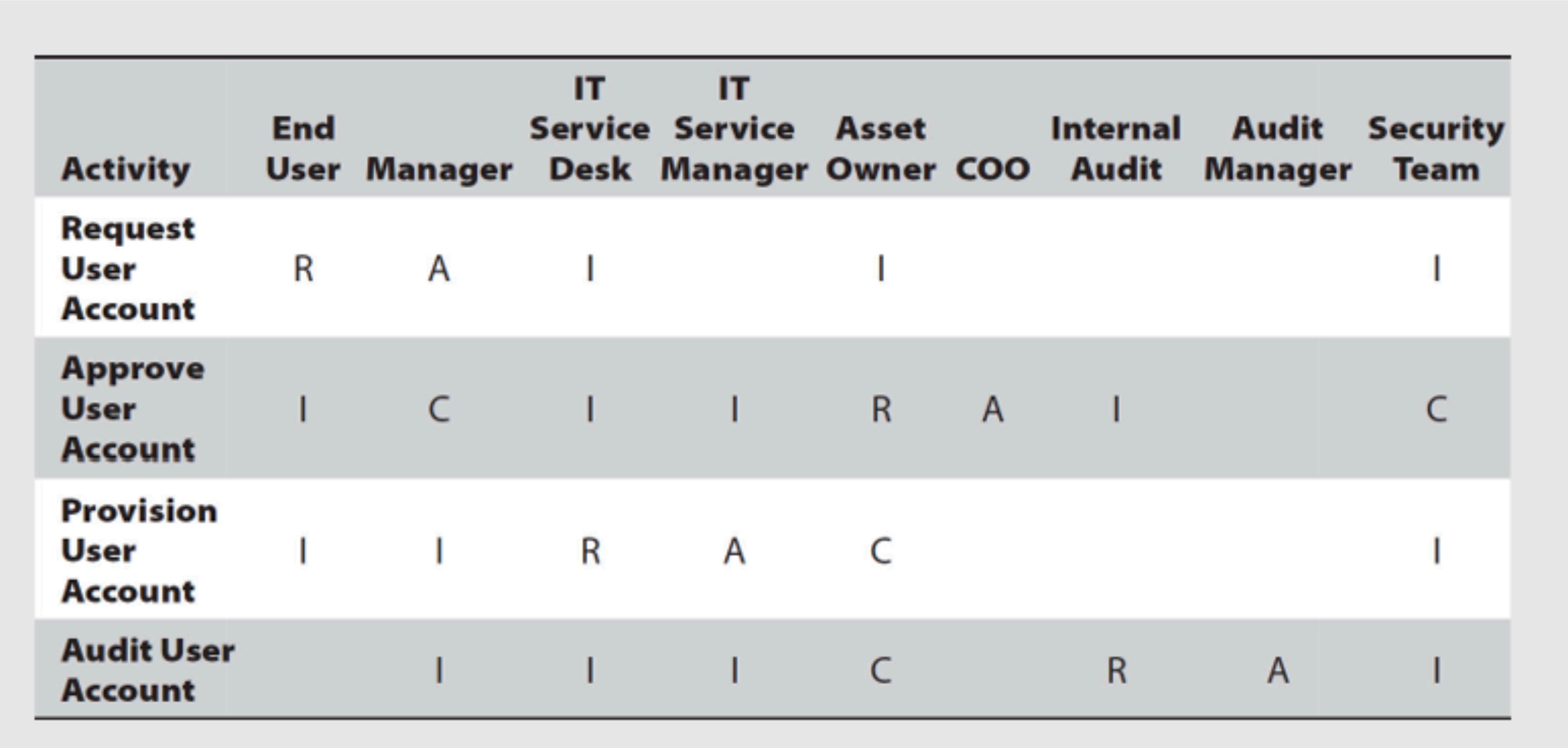
  - **Understand and conform to information security policy, harassment policy, and other policies**
  - **Understand and conform to code of ethics and behavior**

RACI Charts



Activity	Responsible	Accountable	Consulted	Informed
Request User Account	End user	End user manager	IT service desk End user manager	Asset owner Security team
Approve User Account	Asset owner	COO	End user manager Security team	End user Internal audit IT service desk
Provision User Account	IT service desk	IT service manager	Asset owner	End user End user manager Security team
Audit User Account	Internal auditor	Internal audit manager	Asset owner	IT service desk IT service manager End user manager

RACI Charts



Activity	End User	Manager	IT Service Desk	IT Service Manager	Asset Owner	COO	Internal Audit	Audit Manager	Security Team
Request User Account	R	A	I		I				I
Approve User Account	I	C	I	I	R	A	I		C
Provision User Account	I	I	R	A	C				I
Audit User Account		I	I	I	C		R	A	I

Considerations

- **When assigning roles in a RACI chart**
  - **Skills**
  - **Segregation of duties**
  - **Conflict of interest**

Kahoot!

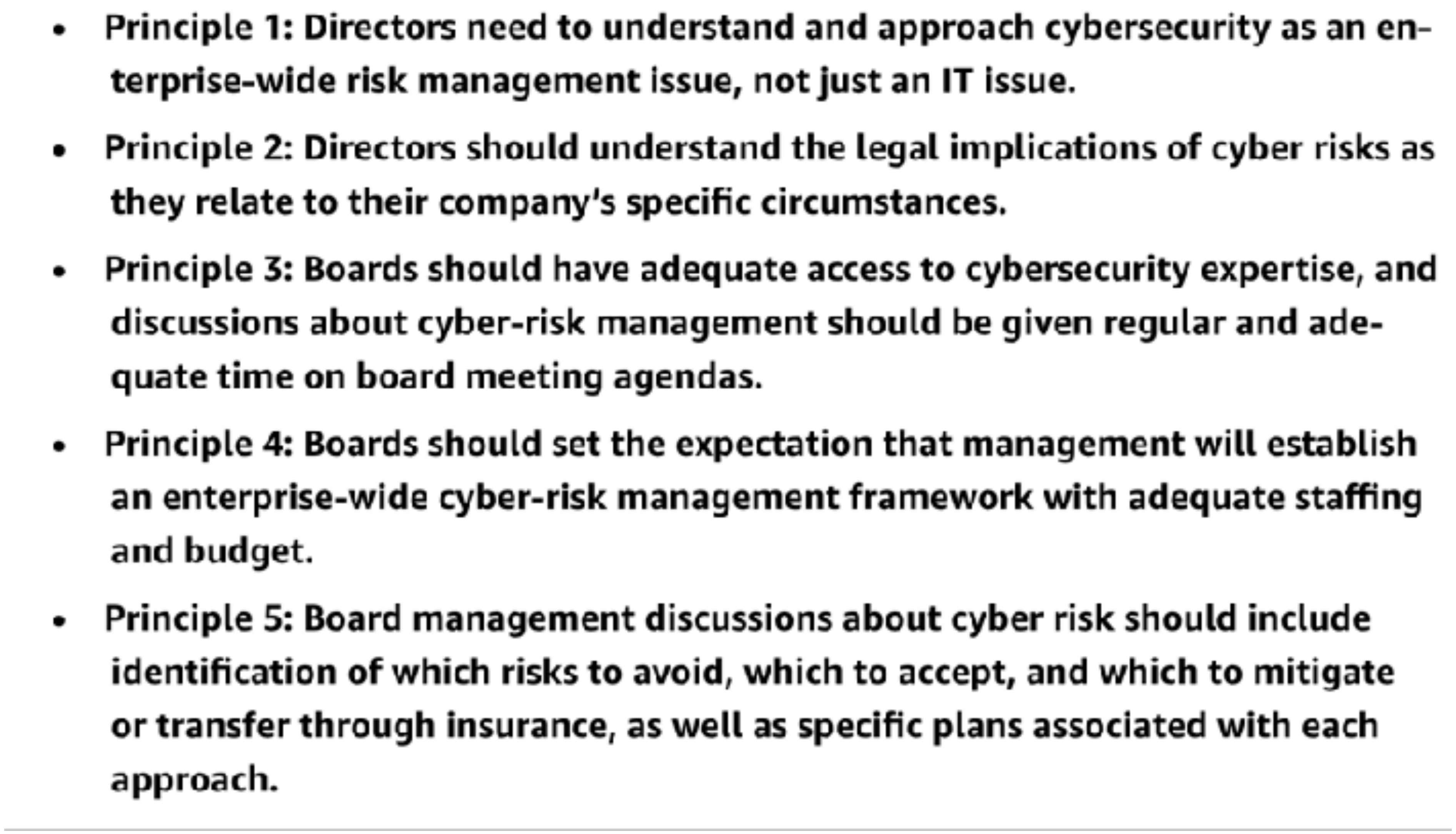
Ch 2a-1

Board of Directors

- **Fiduciary duty**
    - **Accountable to shareholders to act in the best interests of the organization**
- **Selected for**
    - **Investor representation**
    - **Business experience**
    - **Access to resources**
- **Appoints the CEO**

Five Principles

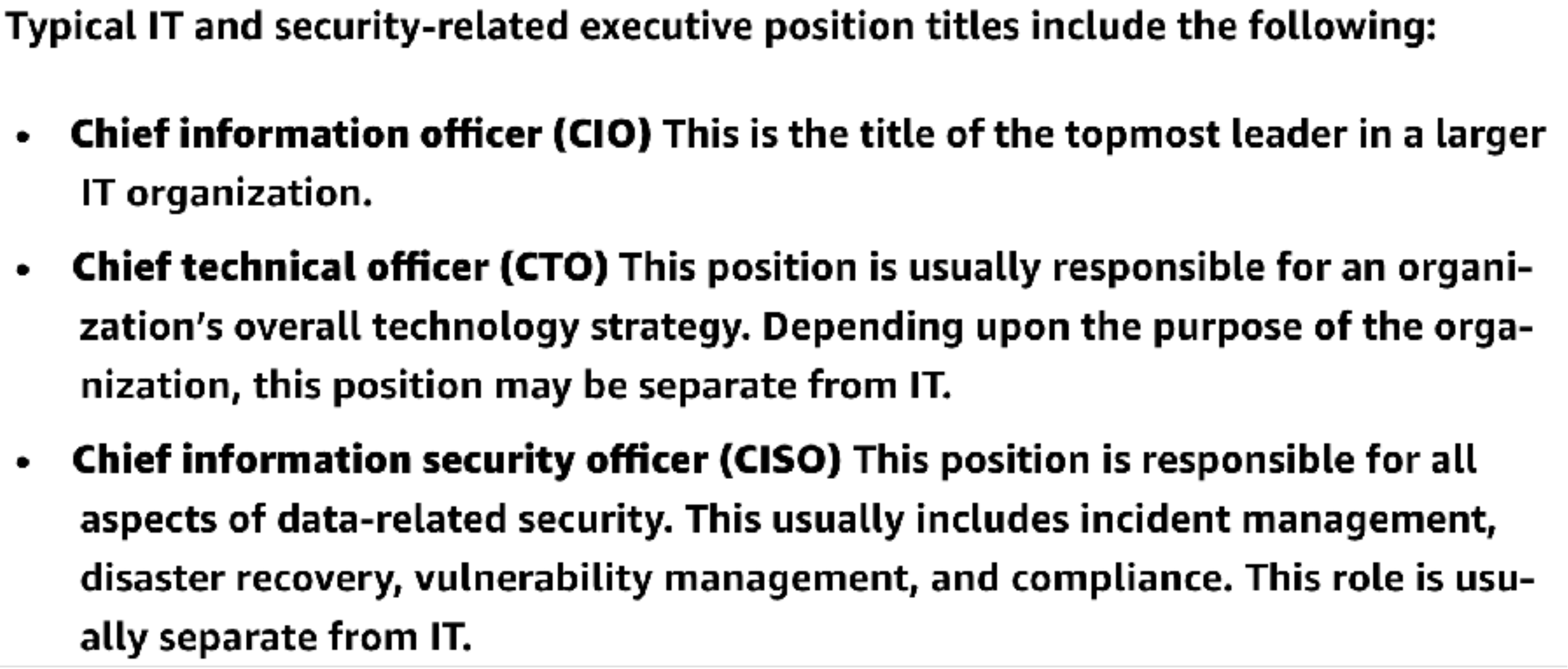
- **From National Association of Corporate Directors**



- **Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.**
- **Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.**
- **Principle 3: Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.**
- **Principle 4: Boards should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.**
- **Principle 5: Board management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.**

Executive Management

- **Carries out directives from the board of directors**



Typical IT and security-related executive position titles include the following:

- **Chief information officer (CIO)** This is the title of the topmost leader in a larger IT organization.
- **Chief technical officer (CTO)** This position is usually responsible for an organization's overall technology strategy. Depending upon the purpose of the organization, this position may be separate from IT.
- **Chief information security officer (CISO)** This position is responsible for all aspects of data-related security. This usually includes incident management, disaster recovery, vulnerability management, and compliance. This role is usually separate from IT.

Executive Management

- **Ratifies corporate security policy**
  - **Publicly supporting it**
- **Leads by example**
- **Has ultimate responsibility**

Security Steering Committee's Responsibilities

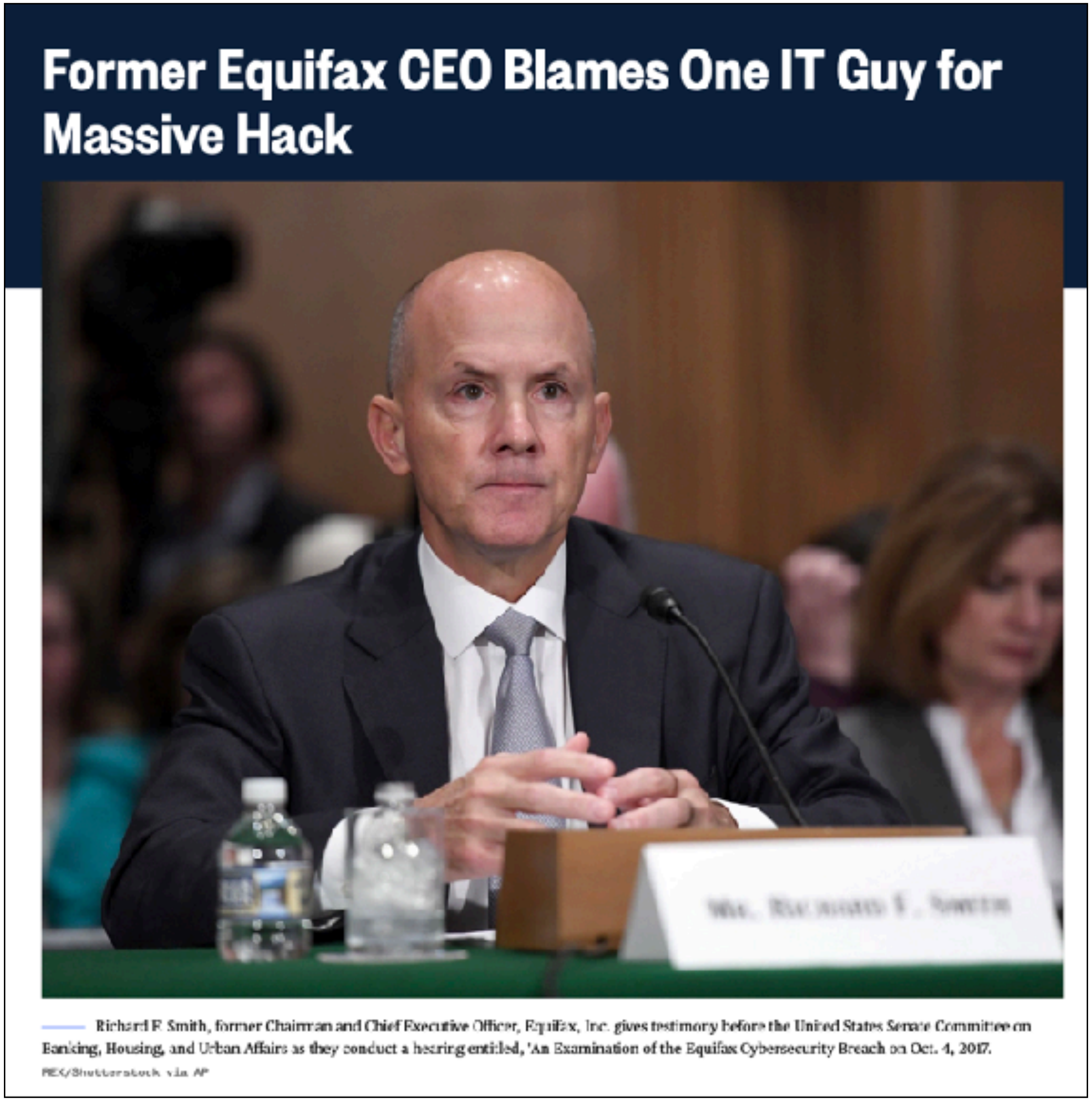
- **Risk treatment deliberation and recommendation**
- **Discussion and coordination of IT and security projects**
- **Review of recent risk assessments**
- **Discussion of new laws, regulations, and requirements**
- **Review of recent security incidents**

Business Process and Business Asset Owners

- **Usually nontechnical personnel**
- **Responsibilities:**
  - **Access grants, revocation, and reviews**
  - **Configuration**
  - **Function definition**
  - **Process definition**
  - **Physical location**

Custodial Responsibilities

- **IT staff acts as a proxy for asset owners**
- **Should implement decisions from the asset owner**
- **But often the asset owner is uninvolved and uninformed, instead of periodically reviewing these decisions**



Former Equifax CEO Blames One IT Guy for Massive Hack

Richard F. Smith, former Chairman and Chief Executive Officer, Equifax, Inc. gives testimony before the United States Senate Committee on Banking, Housing, and Urban Affairs as they conduct a hearing entitled, 'An Examination of the Equifax Cybersecurity Breach on Oct. 4, 2017.

REX/Shutterstock via AP

- **https://www.nbcnews.com/business/consumer/former-equifax-ceo-blames-one-it-guy-massive-hack-n807956**

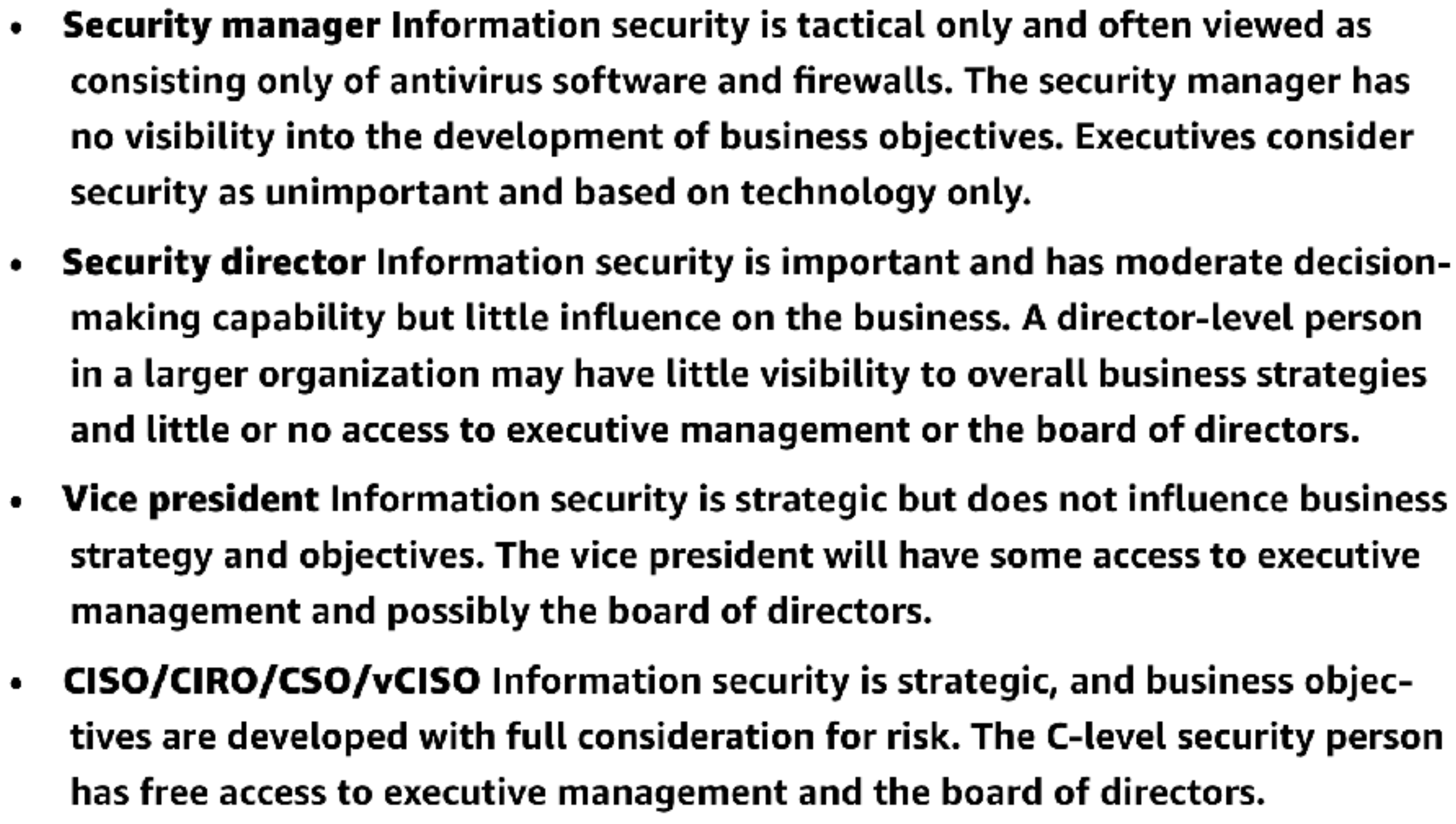
Chief Information Security Officer (CISO)

- **Highest-ranking security person**
- **Develops security strategies**
- **Similar titles**
  - **Chief Security Officer (CSO)**
  - **Chief Information Risk Officer (CIRO)**
  - **Chief Risk Officer (CRO)**

Position of CISO

- **Reports to Chief Operating Officer (COO) or Chief Executive Officer (CEO)**
  - **Sometimes to CIO or legal or someone else**
- **Many organizations lack a CISO but have a manager of information security lower on the org chart, weakening security posture**
- **Small to medium-sized orgs may contract with a virtual CISO for strategy and planning**

Rank Sets Tone and Gives Power



- **Security manager** Information security is tactical only and often viewed as consisting only of antivirus software and firewalls. The security manager has no visibility into the development of business objectives. Executives consider security as unimportant and based on technology only.
- **Security director** Information security is important and has moderate decision-making capability but little influence on the business. A director-level person in a larger organization may have little visibility to overall business strategies and little or no access to executive management or the board of directors.
- **Vice president** Information security is strategic but does not influence business strategy and objectives. The vice president will have some access to executive management and possibly the board of directors.
- **CISO/CIRO/CSO/vCISO** Information security is strategic, and business objectives are developed with full consideration for risk. The C-level security person has free access to executive management and the board of directors.

Chief Privacy Officer

- **For organization with large amounts of customer Personally Identifiable Information (PII)**
- **Regulations like**
  - **Health Insurance Portability and Accountability Act (HIPAA)**
  - **Fair Credit Reporting Act (FRCA)**
  - **The Gramm-Leach-Bliley Act (GLBA)**

Software Development

- **Systems architect**
- **Systems analyst**
- **Software engineer/developer**
- **Software tester**

Data Management

- Data manager
- Database architect
- Big data architect
- Database administrator (DBA)
- Database analyst
- Data scientist

Network Management

- **Network architect**
- **Network engineer**
- **Network administrator**
- **Telecom engineer**

Systems Management

- **Systems architect**
- **Systems analyst**
- **Storage engineer**
- **Systems administrator**

Operations

- **Operations manager**
- **Operations analyst**
- **Controls analyst**
- **Systems operator**
- **Data entry**
- **Media manager**

Security Operations

- **Security architect**
- **Security engineer**
- **Security analyst**
  - **Examines logs**
- **Access administrator**

Security Audit

- **Security audit manager**
- **Security auditor**

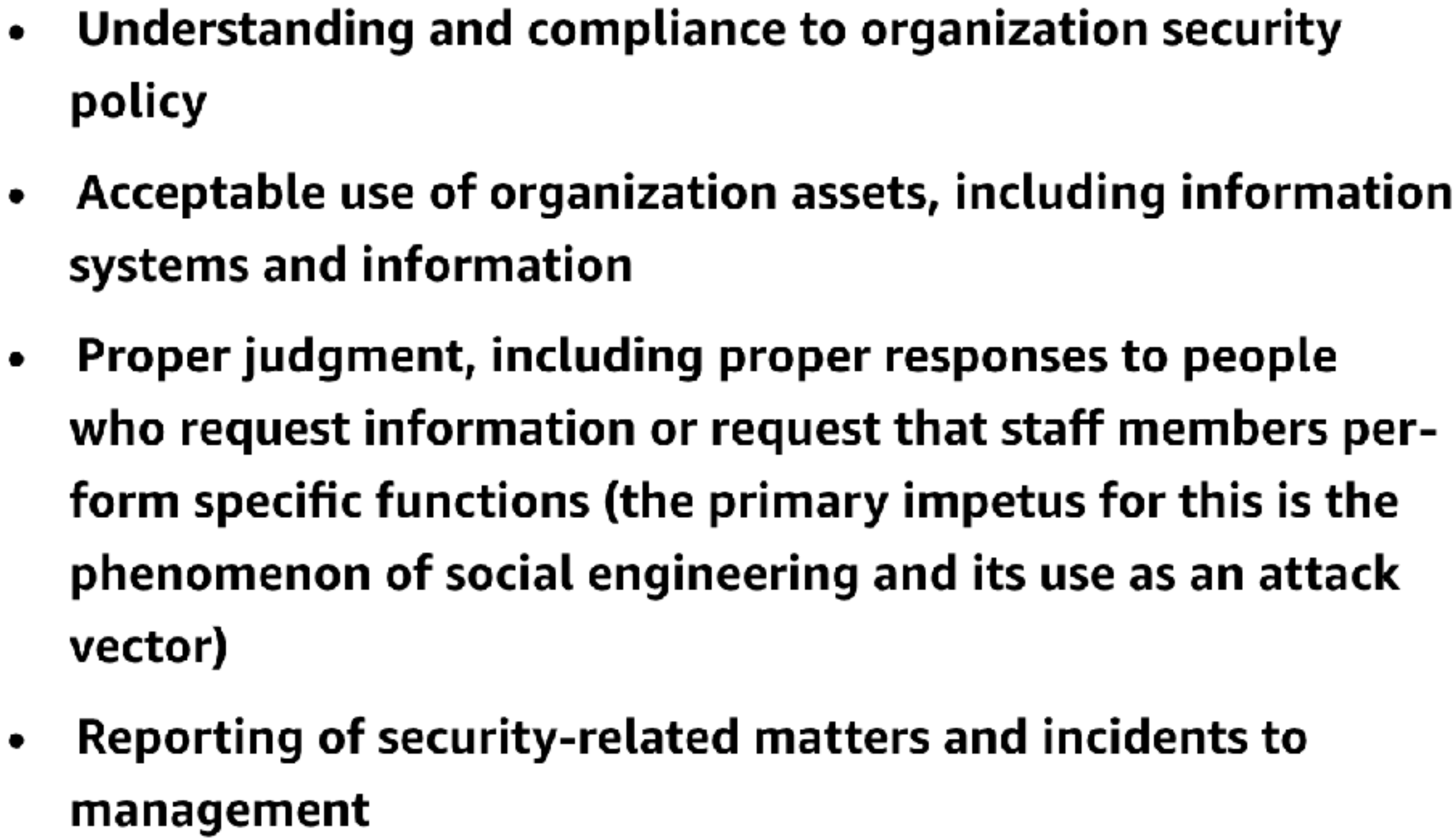
Service Desk

- **Service desk manager**
- **Service desk analyst**
- **Technical support analyst**

Quality Assurance & Other Roles

- **QA manager**
- **QC manager**
- **Vendor manager**
- **Project manager**

General Staff Security Responsibilities



- Understanding and compliance to organization security policy
- Acceptable use of organization assets, including information systems and information
- Proper judgment, including proper responses to people who request information or request that staff members perform specific functions (the primary impetus for this is the phenomenon of social engineering and its use as an attack vector)
- Reporting of security-related matters and incidents to management

Monitoring Responsibilities

- **Confirming that the correct jobs are being carried out in the correct way**
  - **Controls and internal audit**
  - **Metrics and reporting**
  - **Work measurement**
  - **Performance evaluation**
  - **360 feedback -- from peers, subordinates, and management**
  - **Position benchmarking -- comparing job titles with other organizations**

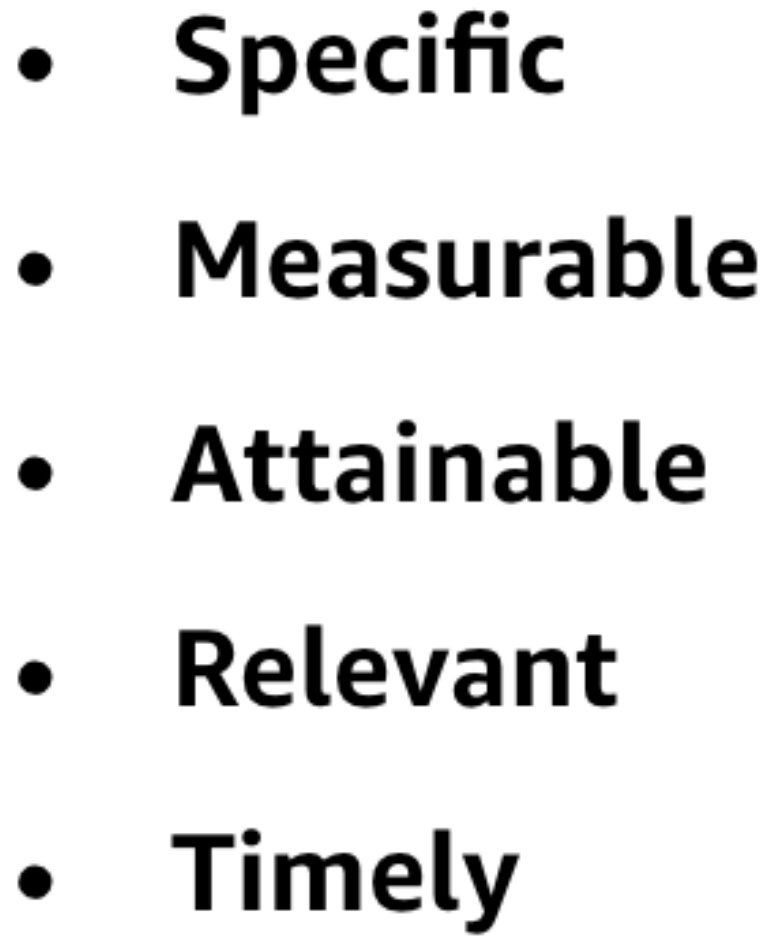
Information Security Governance Metrics

- **Technical metrics, counts of events from**
  - **Firewall, IDS, Anti-malware, DLP, etc.**
- **Business-related metrics**
  - **Key Risk Indicators (KRIs)**
  - **Key Goal Indicators (KGIs)**
  - **Key Performance Indicators (KPIs)**

Return on Security Investment

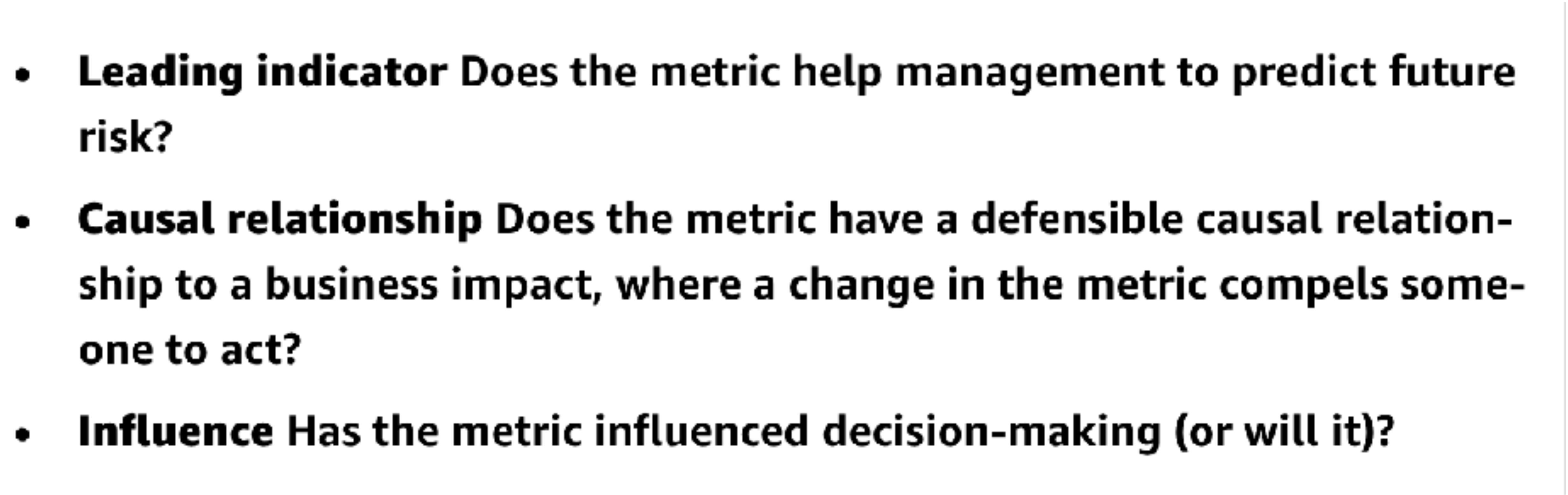
- **Difficult to quantify**
- **Because breaches are rare**
- **Other ways to justify security**
  - **Fiduciary responsibility**
  - **Regulation**
  - **Competitive differentiation**

SMART Metrics



- Specific
- Measurable
- Attainable
- Relevant
- Timely

Good Considerations for Metrics

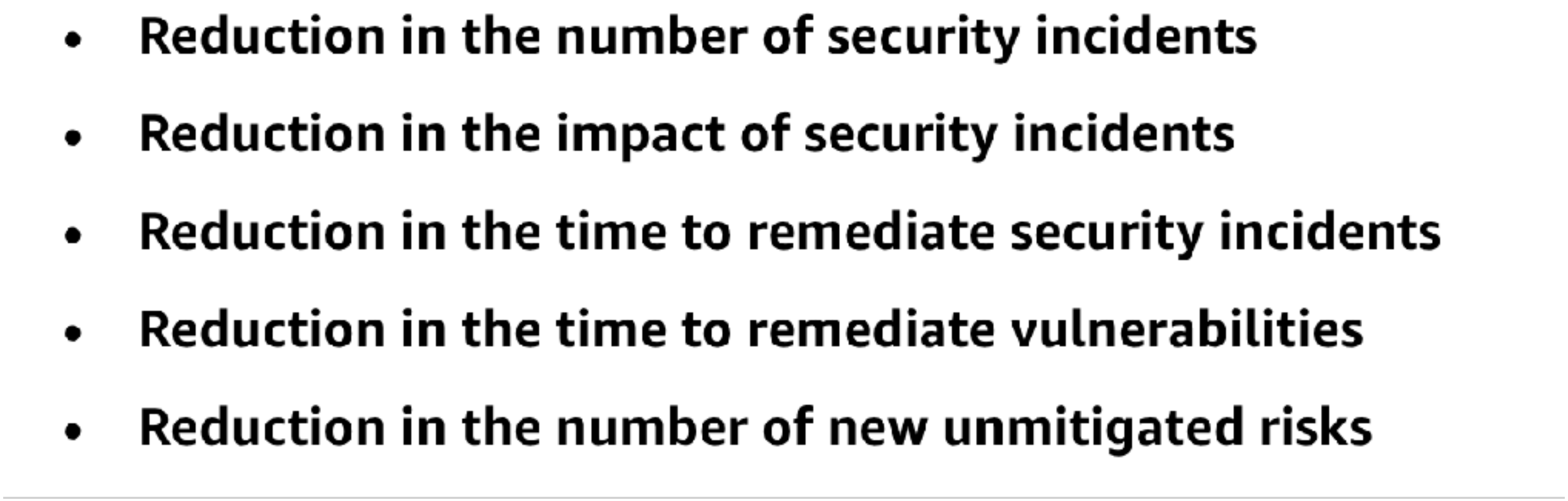


- **Leading indicator** Does the metric help management to predict future risk?
- **Causal relationship** Does the metric have a defensible causal relationship to a business impact, where a change in the metric compels someone to act?
- **Influence** Has the metric influenced decision-making (or will it)?

Kahoot!

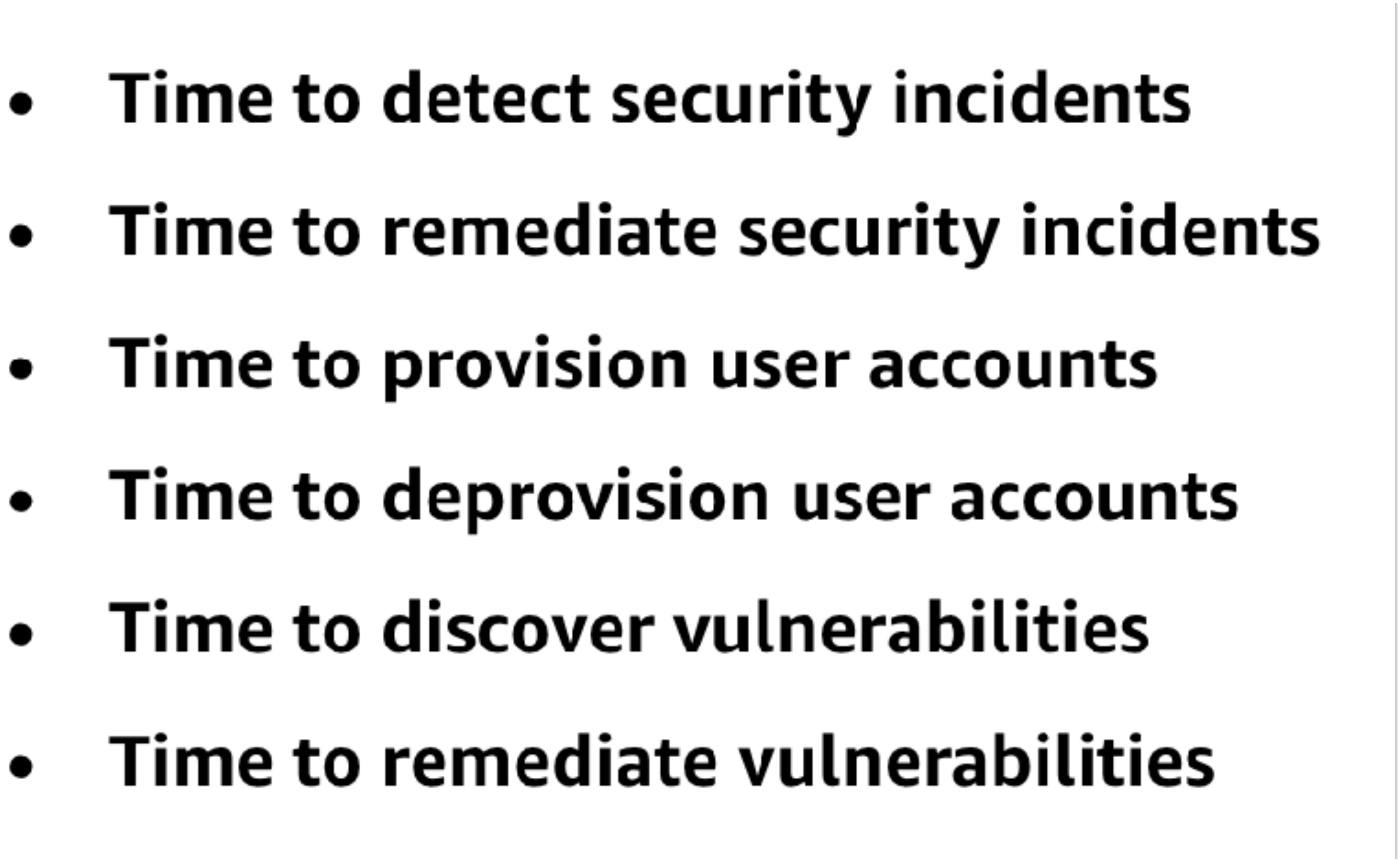
Ch 2a-1

Risk Management



- Reduction in the number of security incidents
- Reduction in the impact of security incidents
- Reduction in the time to remediate security incidents
- Reduction in the time to remediate vulnerabilities
- Reduction in the number of new unmitigated risks

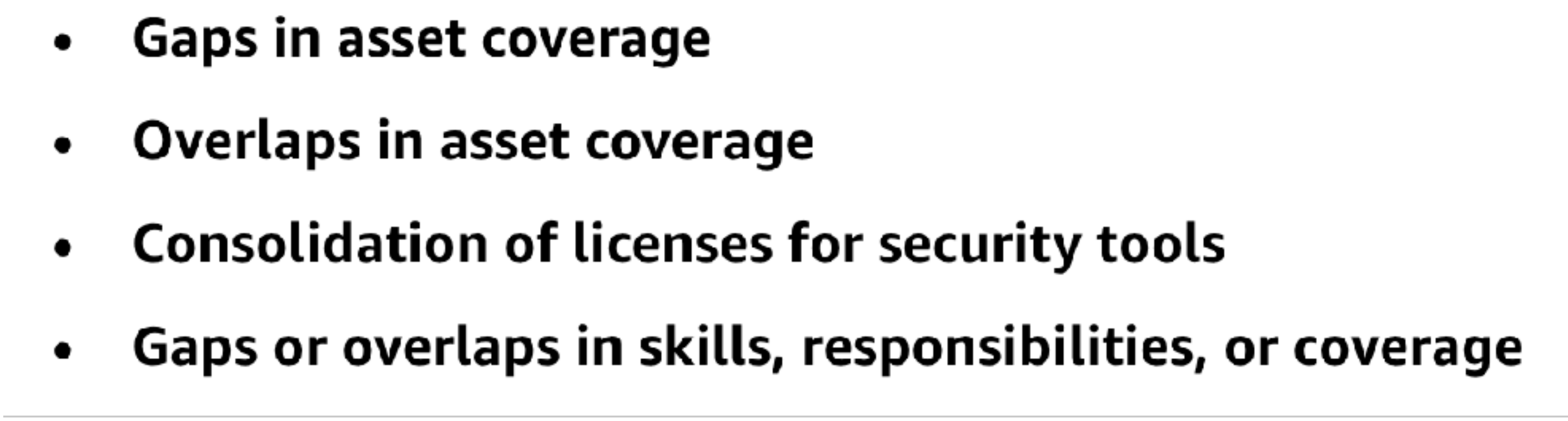
Performance Measurement



- Time to detect security incidents
- Time to remediate security incidents
- Time to provision user accounts
- Time to deprovision user accounts
- Time to discover vulnerabilities
- Time to remediate vulnerabilities

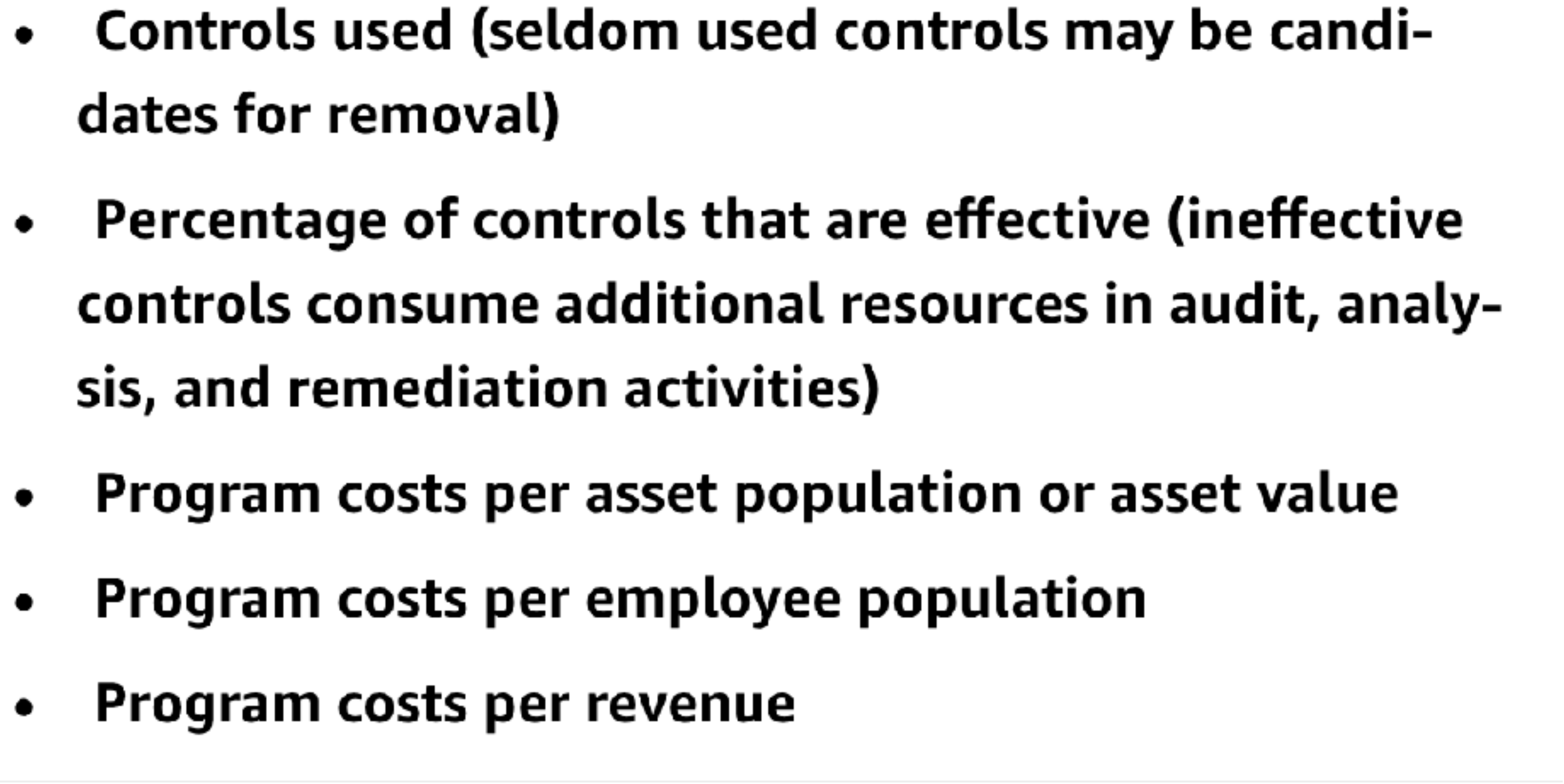
Convergence Metrics

- **Large organizations with multiple business units or locations**



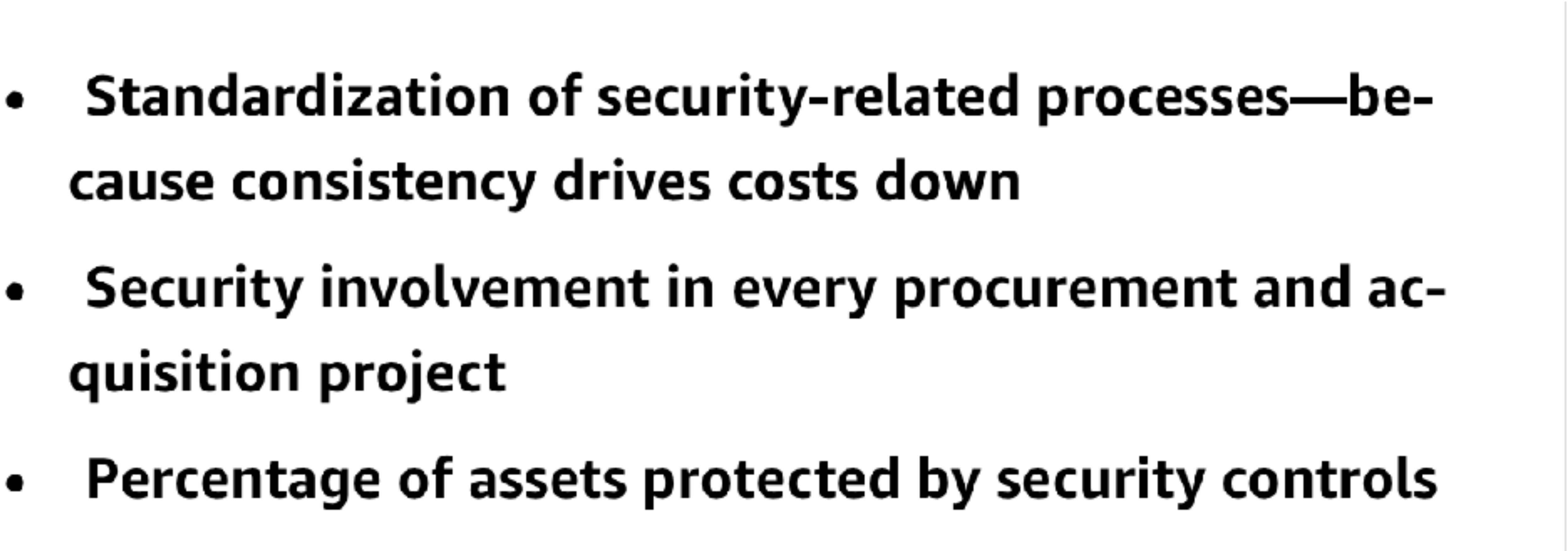
- **Gaps in asset coverage**
- **Overlaps in asset coverage**
- **Consolidation of licenses for security tools**
- **Gaps or overlaps in skills, responsibilities, or coverage**

Value Delivery Metrics



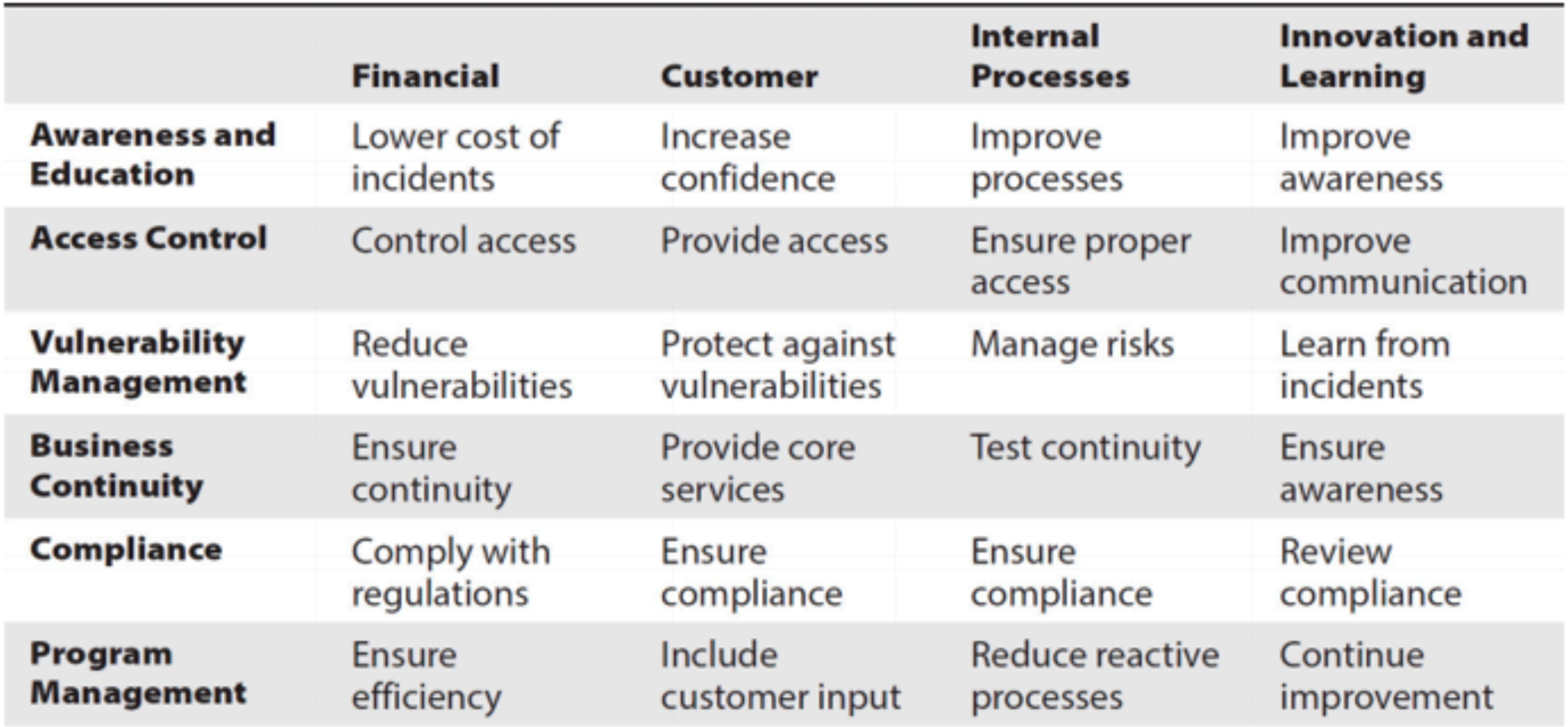
- Controls used (seldom used controls may be candidates for removal)
- Percentage of controls that are effective (ineffective controls consume additional resources in audit, analysis, and remediation activities)
- Program costs per asset population or asset value
- Program costs per employee population
- Program costs per revenue

Resource Management Metrics



- **Standardization of security-related processes—because consistency drives costs down**
- **Security involvement in every procurement and acquisition project**
- **Percentage of assets protected by security controls**

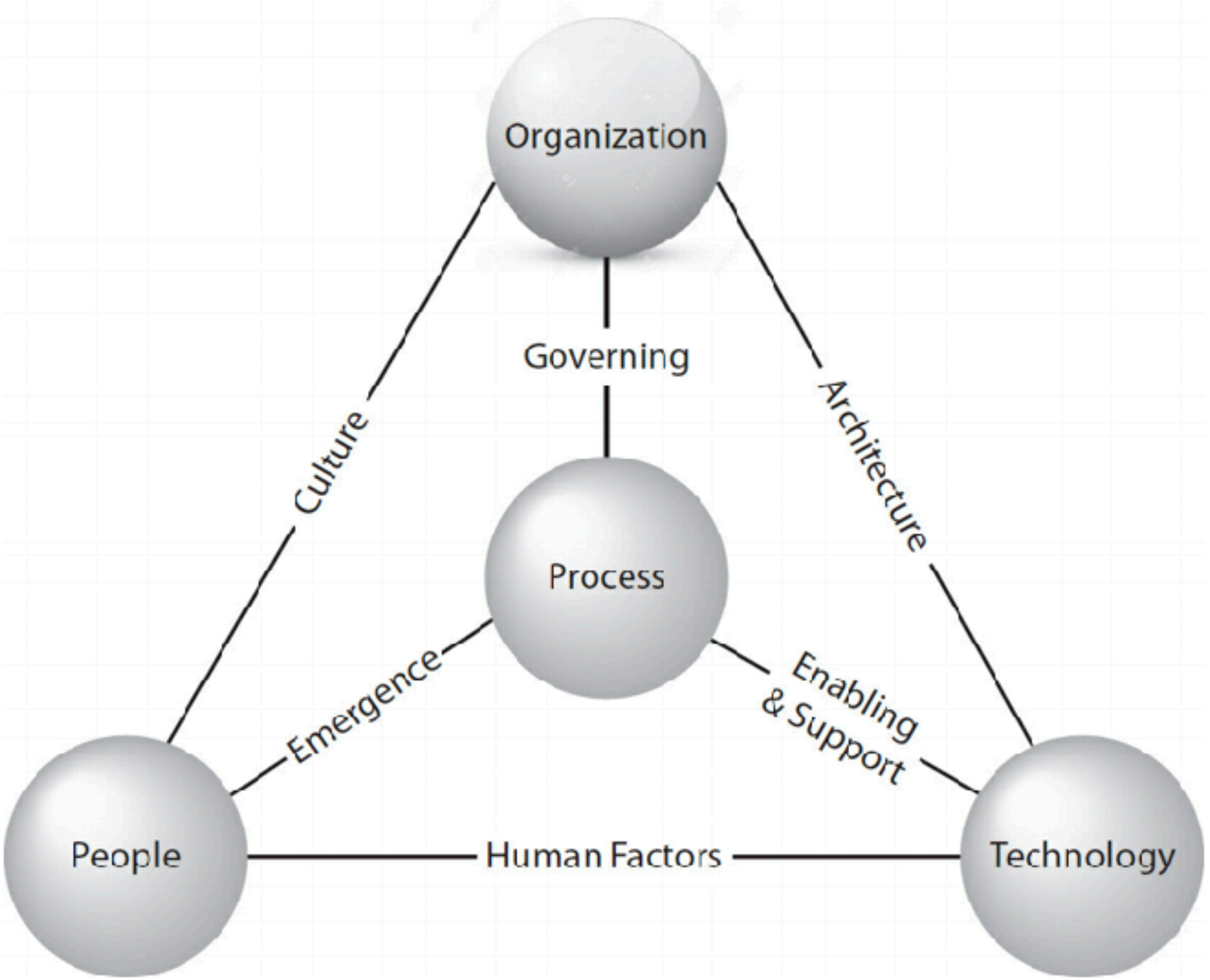
Security Balanced Scorecard



	Financial	Customer	Internal Processes	Innovation and Learning
Awareness and Education	Lower cost of incidents	Increase confidence	Improve processes	Improve awareness
Access Control	Control access	Provide access	Ensure proper access	Improve communication
Vulnerability Management	Reduce vulnerabilities	Protect against vulnerabilities	Manage risks	Learn from incidents
Business Continuity	Ensure continuity	Provide core services	Test continuity	Ensure awareness
Compliance	Comply with regulations	Ensure compliance	Ensure compliance	Review compliance
Program Management	Ensure efficiency	Include customer input	Reduce reactive processes	Continue improvement

Business Model for Information Security

Business Model for Information Security



BMIS Elements and Dynamic Interconnections

- **Elements**
  - **Organization**
  - **People**
  - **Process**
  - **Technology**

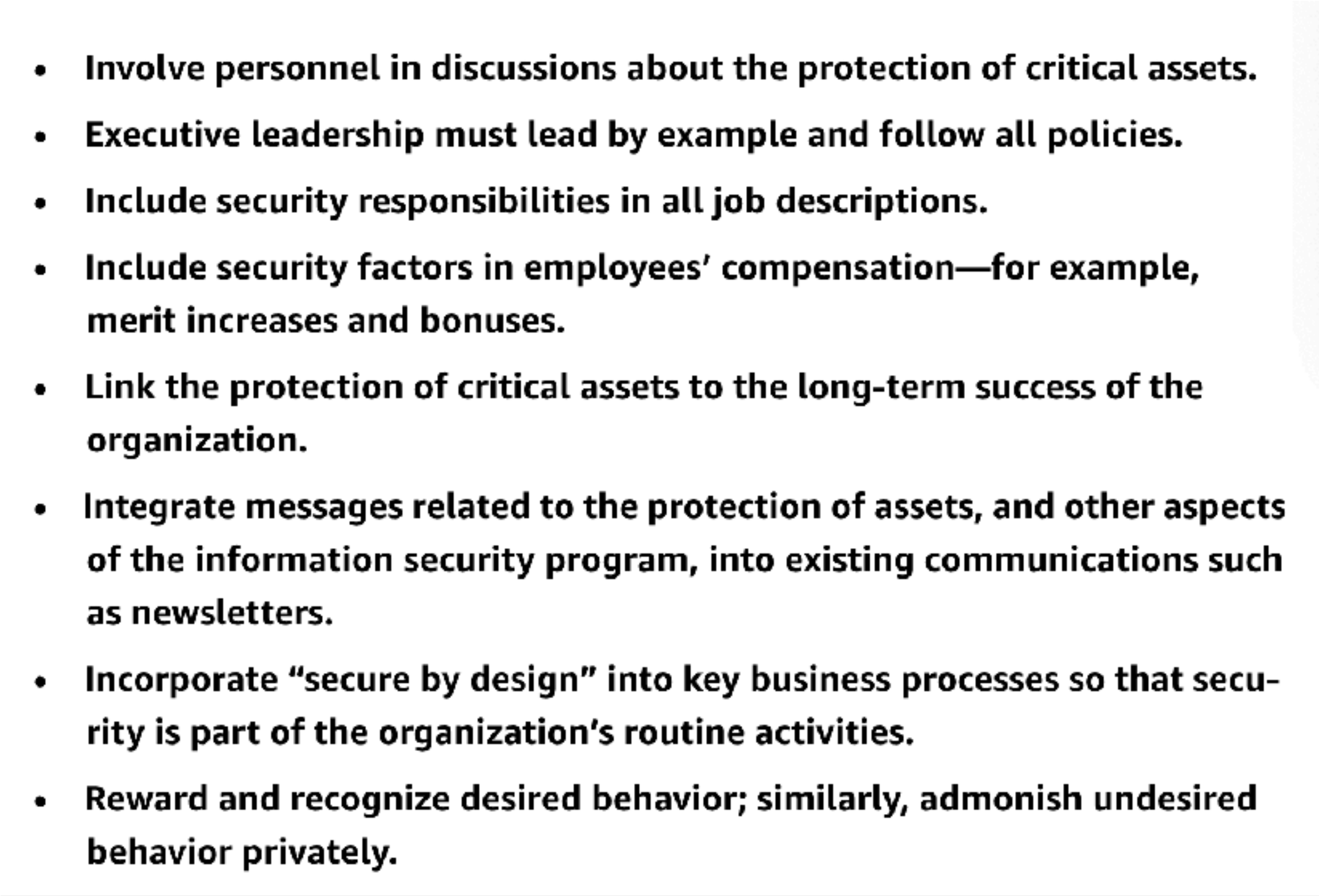
BMIS Elements and Dynamic Interconnections

- **Dynamic Interconnections**
  - **Culture**
  - **Governing**
  - **Architecture**
  - **Emergence**
  - **Enabling and Support**
  - **Human Factors**

Culture

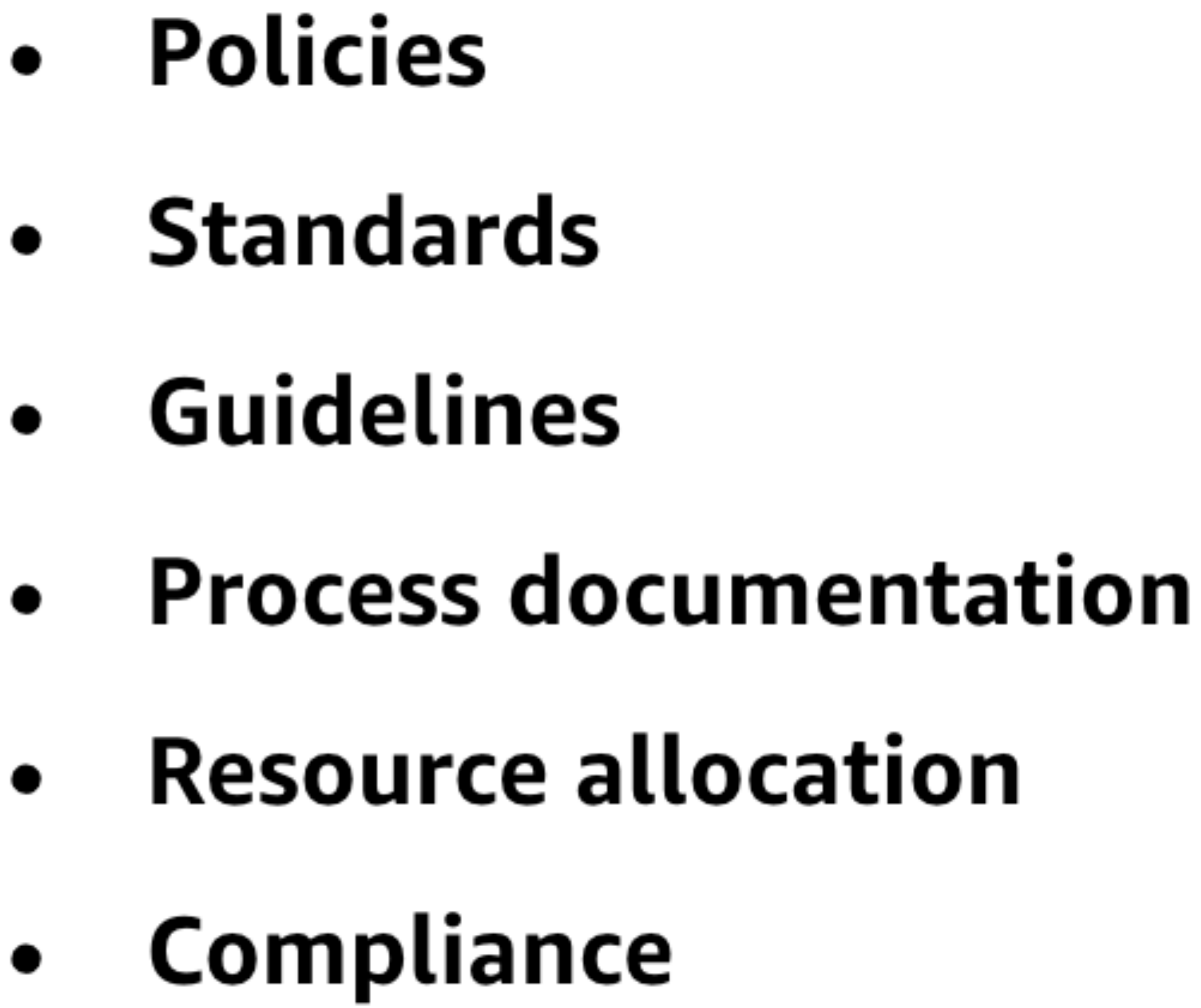
- **"a pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things"**
- **Critical to the success or failure of an information security program**
- **Cannot be legislated or controlled directly**

Steps to Create Favorable Security Culture



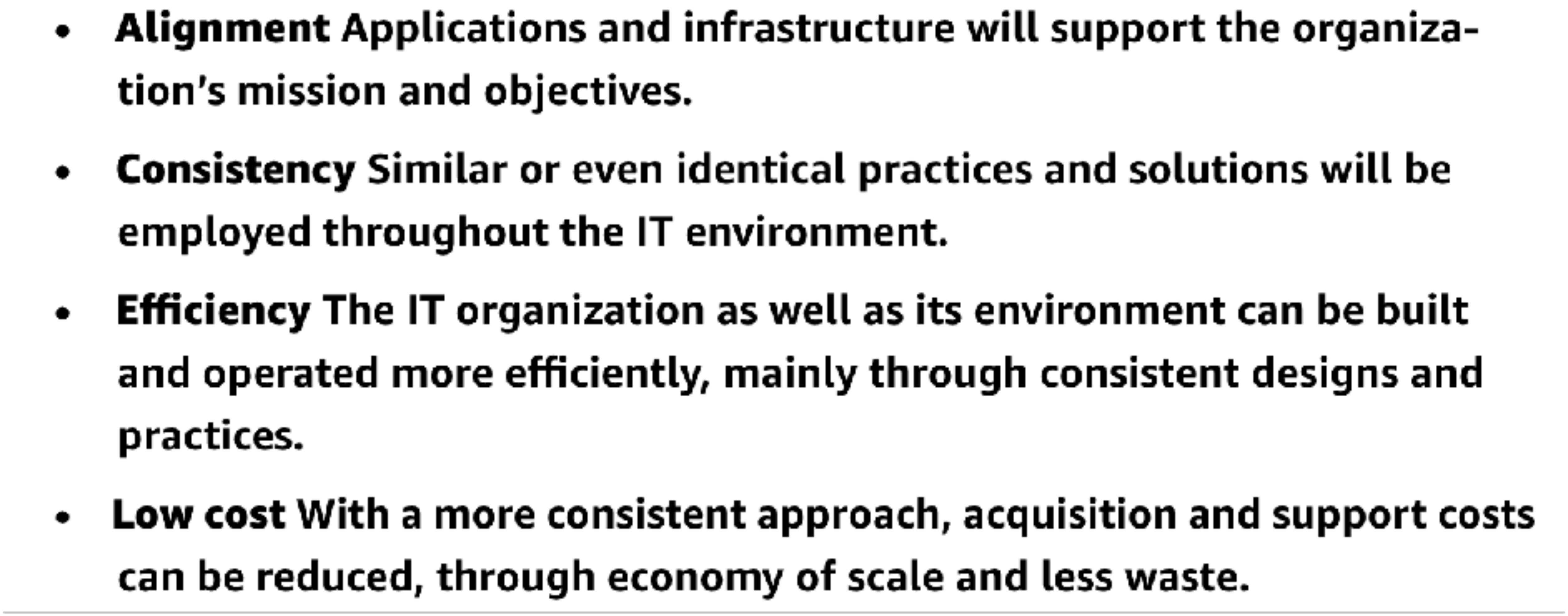
- Involve personnel in discussions about the protection of critical assets.
- Executive leadership must lead by example and follow all policies.
- Include security responsibilities in all job descriptions.
- Include security factors in employees' compensation—for example, merit increases and bonuses.
- Link the protection of critical assets to the long-term success of the organization.
- Integrate messages related to the protection of assets, and other aspects of the information security program, into existing communications such as newsletters.
- Incorporate "secure by design" into key business processes so that security is part of the organization's routine activities.
- Reward and recognize desired behavior; similarly, admonish undesired behavior privately.

Governing



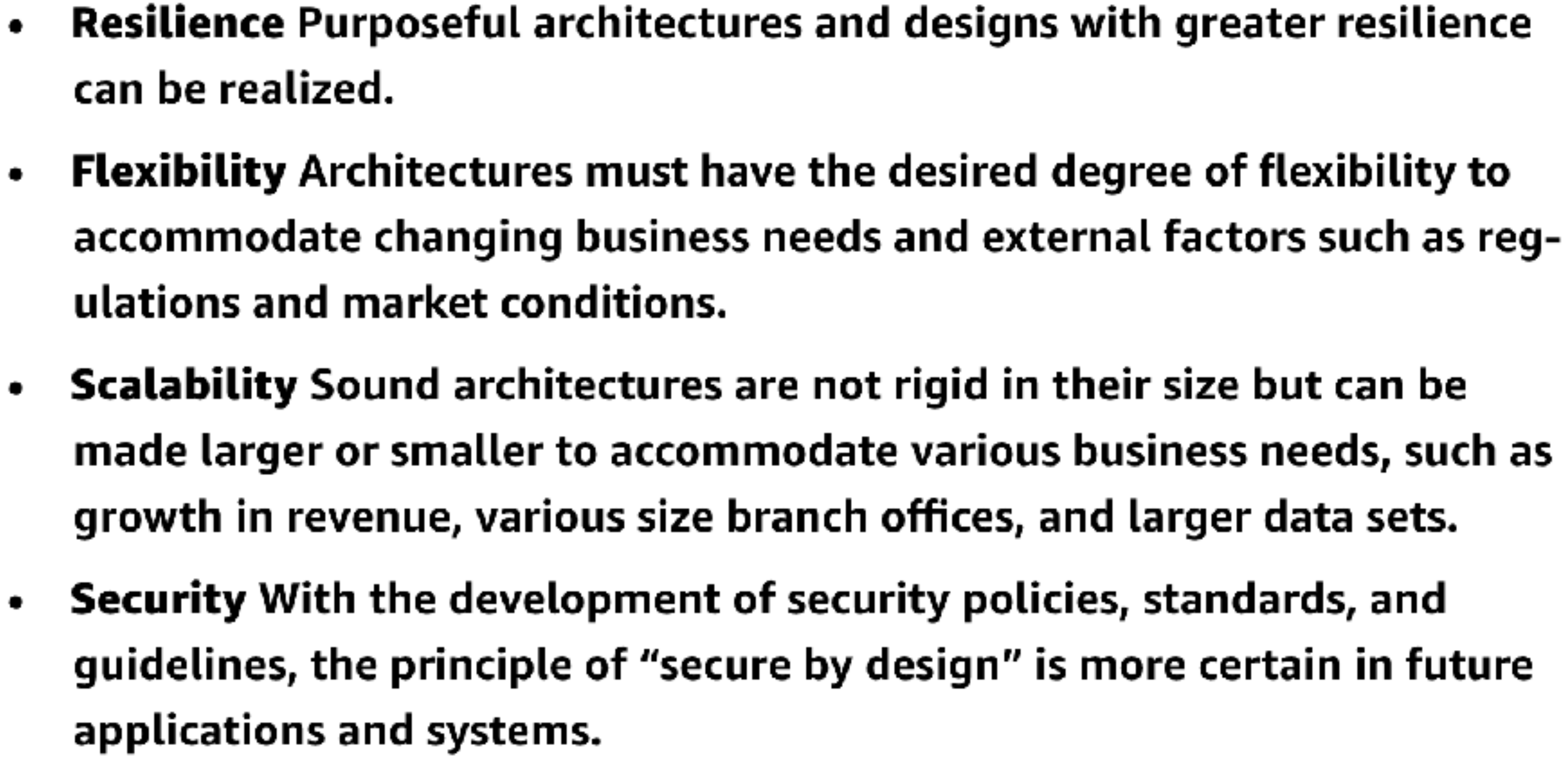
- Policies
- Standards
- Guidelines
- Process documentation
- Resource allocation
- Compliance

Architecture



- **Alignment** Applications and infrastructure will support the organization's mission and objectives.
- **Consistency** Similar or even identical practices and solutions will be employed throughout the IT environment.
- **Efficiency** The IT organization as well as its environment can be built and operated more efficiently, mainly through consistent designs and practices.
- **Low cost** With a more consistent approach, acquisition and support costs can be reduced, through economy of scale and less waste.

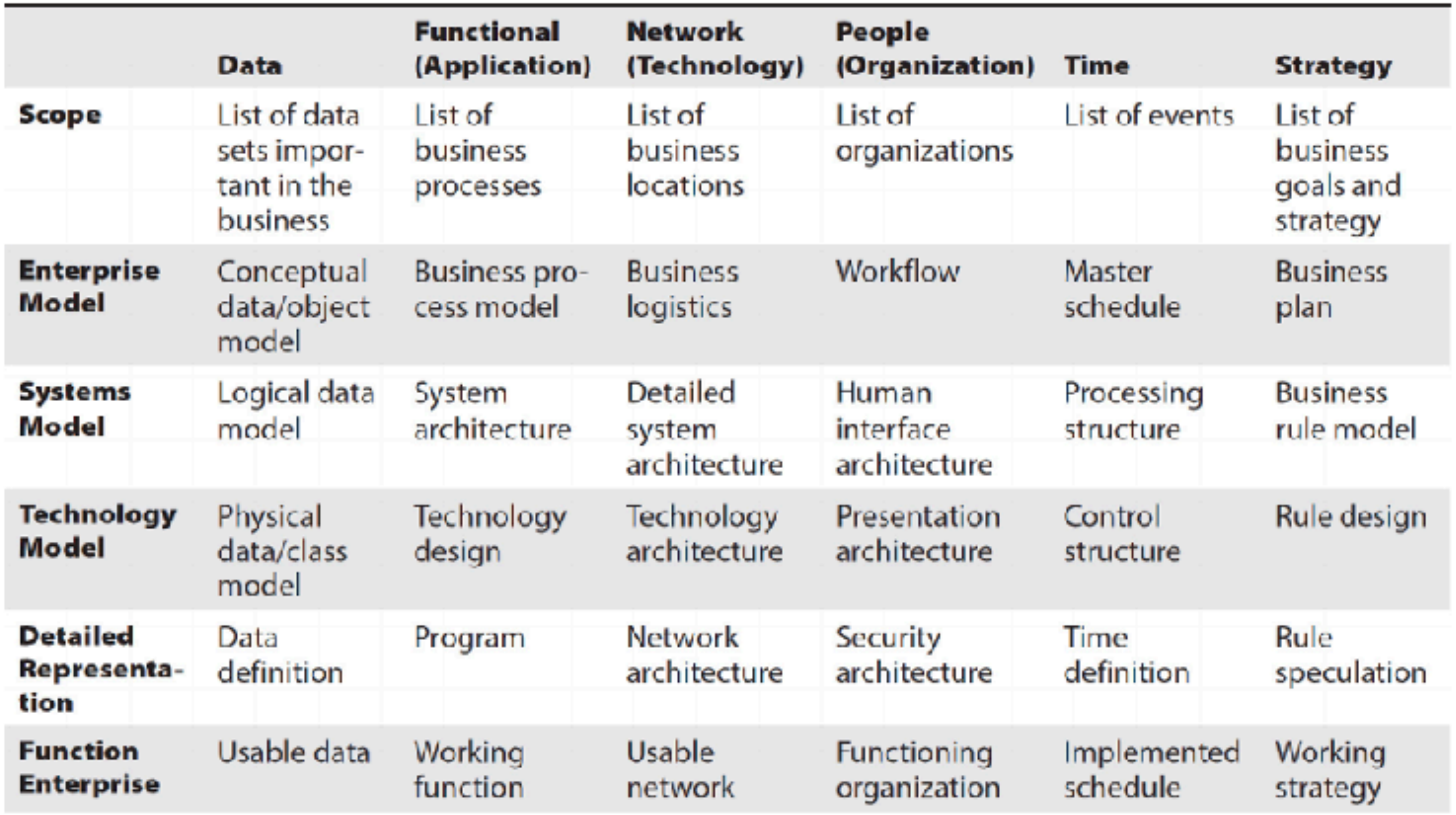
Architecture



- **Resilience** Purposeful architectures and designs with greater resilience can be realized.
- **Flexibility** Architectures must have the desired degree of flexibility to accommodate changing business needs and external factors such as regulations and market conditions.
- **Scalability** Sound architectures are not rigid in their size but can be made larger or smaller to accommodate various business needs, such as growth in revenue, various size branch offices, and larger data sets.
- **Security** With the development of security policies, standards, and guidelines, the principle of “secure by design” is more certain in future applications and systems.

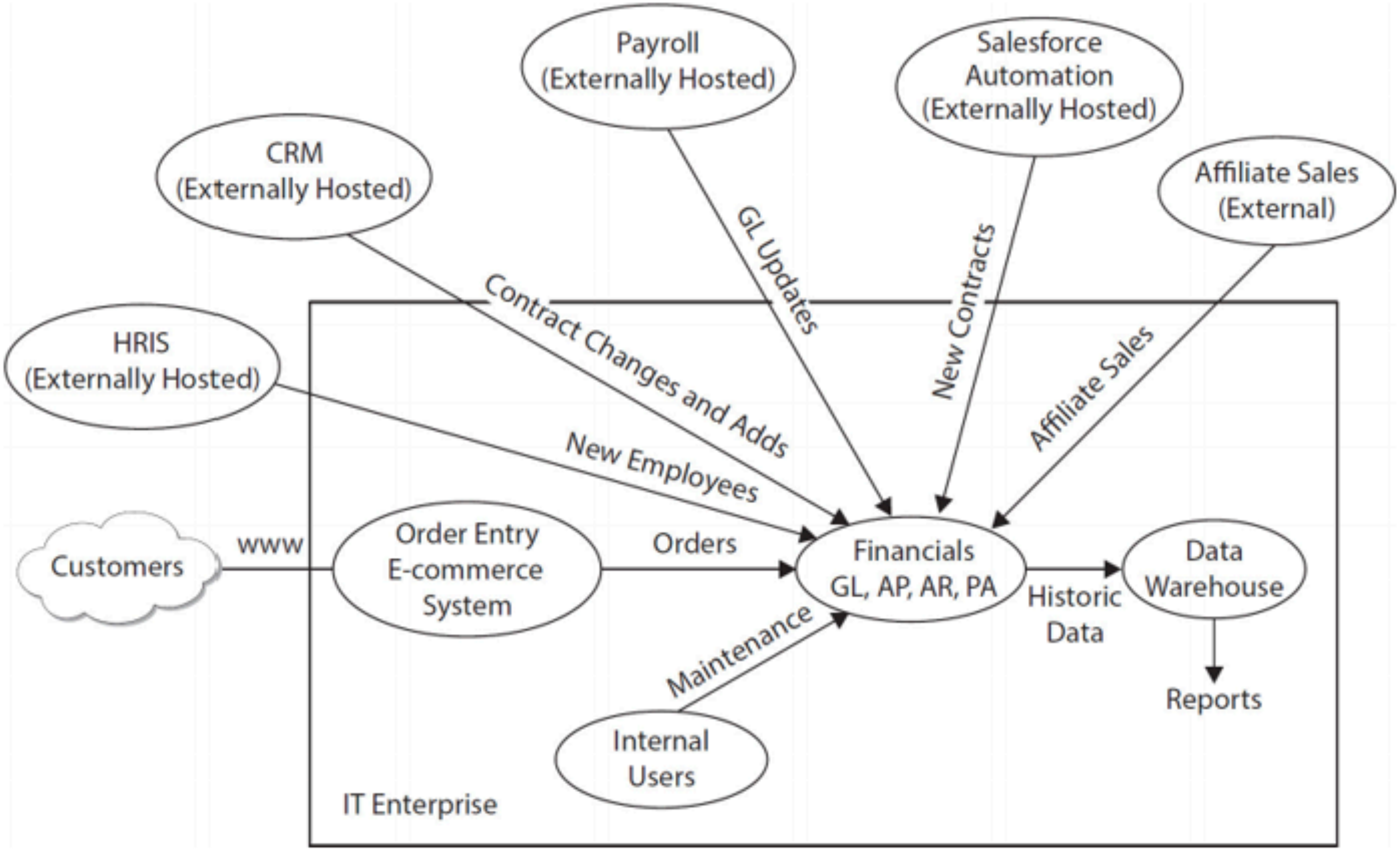
The Zachman Framework

- **The dominant architecture architecture standard**



	Data	Functional (Application)	Network (Technology)	People (Organization)	Time	Strategy
Scope	List of data sets important in the business	List of business processes	List of business locations	List of organizations	List of events	List of business goals and strategy
Enterprise Model	Conceptual data/object model	Business process model	Business logistics	Workflow	Master schedule	Business plan
Systems Model	Logical data model	System architecture	Detailed system architecture	Human interface architecture	Processing structure	Business rule model
Technology Model	Physical data/class model	Technology design	Technology architecture	Presentation architecture	Control structure	Rule design
Detailed Representation	Data definition	Program	Network architecture	Security architecture	Time definition	Rule speculation
Function Enterprise	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Data Flow Diagram



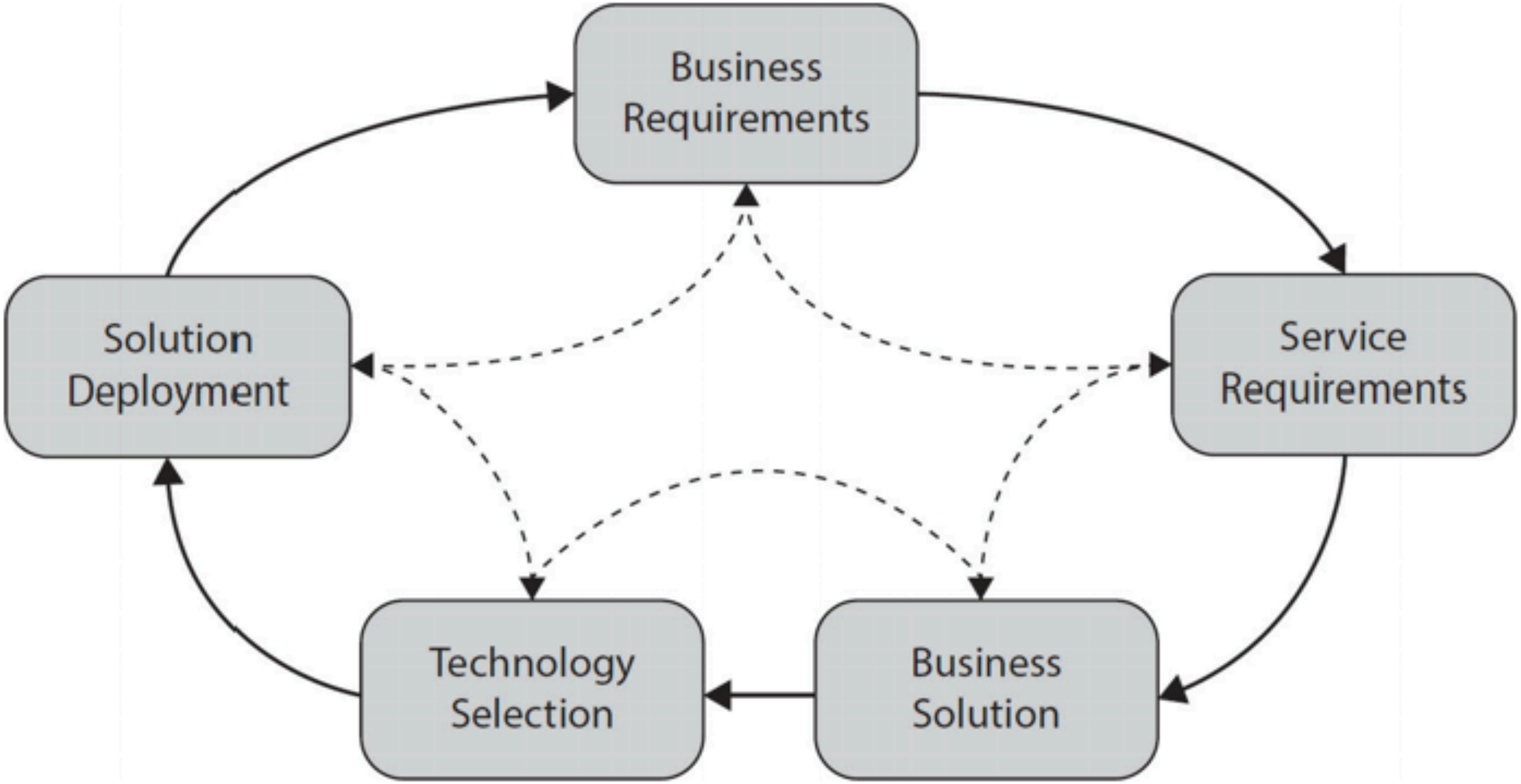
Emergence

- People learning to do things better
- Can lead to improvements, but also cause inconsistent results

Enabling and Support

- **Technology and business people don't understand one another**
- **To fill this gap, create a *requirements document***
  - **Charts listing required and desired functionality for new technologies**

BMIS Enabling and Support Life Cycle



Human Factors

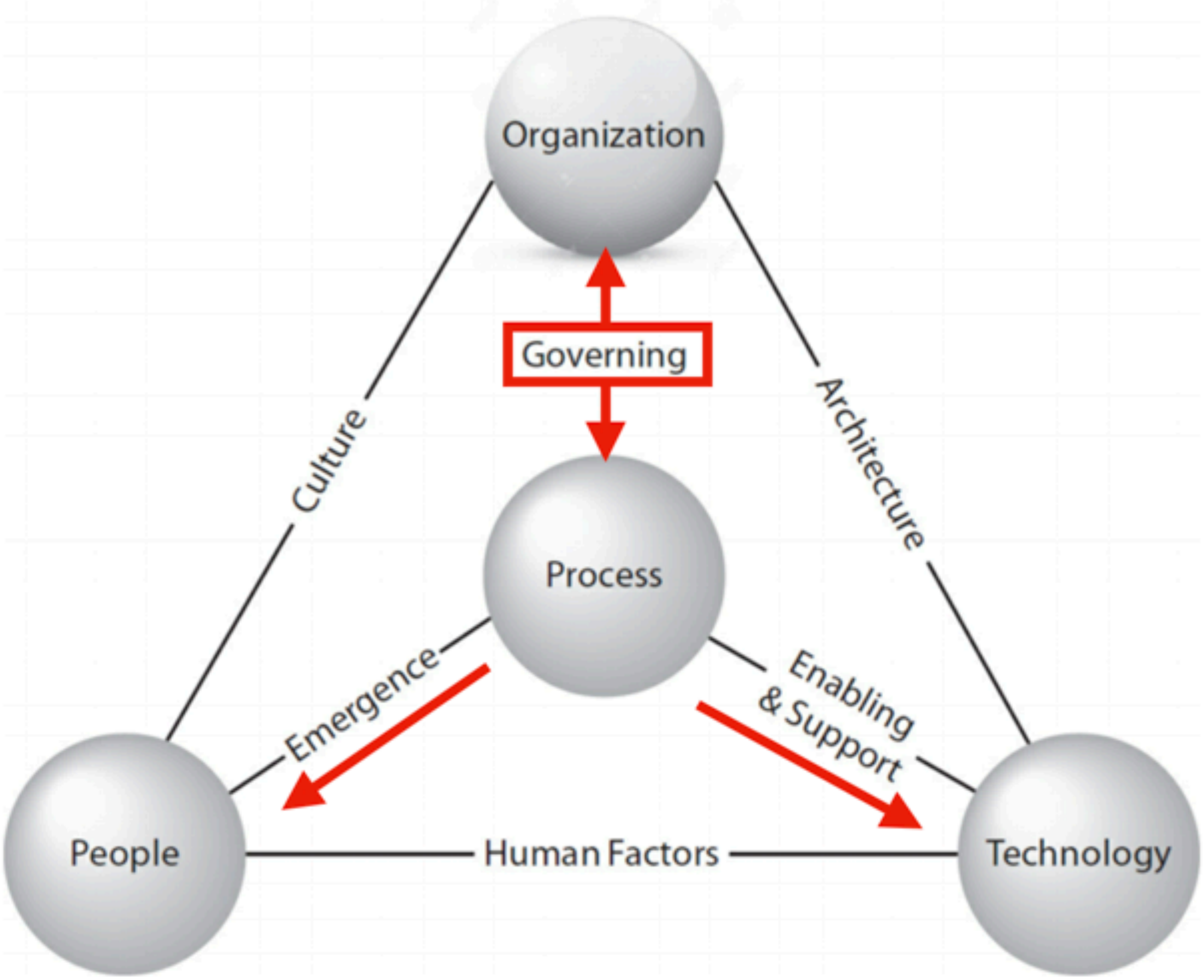
- **Also called *Human-Computer Interaction (HCI)***
- **Includes *User Interface (UI)***

Human Factors

- **Consistency with other systems**
- **Typing and data entry methods**
- **Display and readability**
- **Error recovery**
- **Sound**
- **Voice and biometric recognition**
- **Ergonomics**
- **Environment**

Example 1:
Adverse Effects of a Policy Change

- **New policy regarding personal devices and company email**
- **Affects organization and processes**
- **Changed processes affect people and technology**

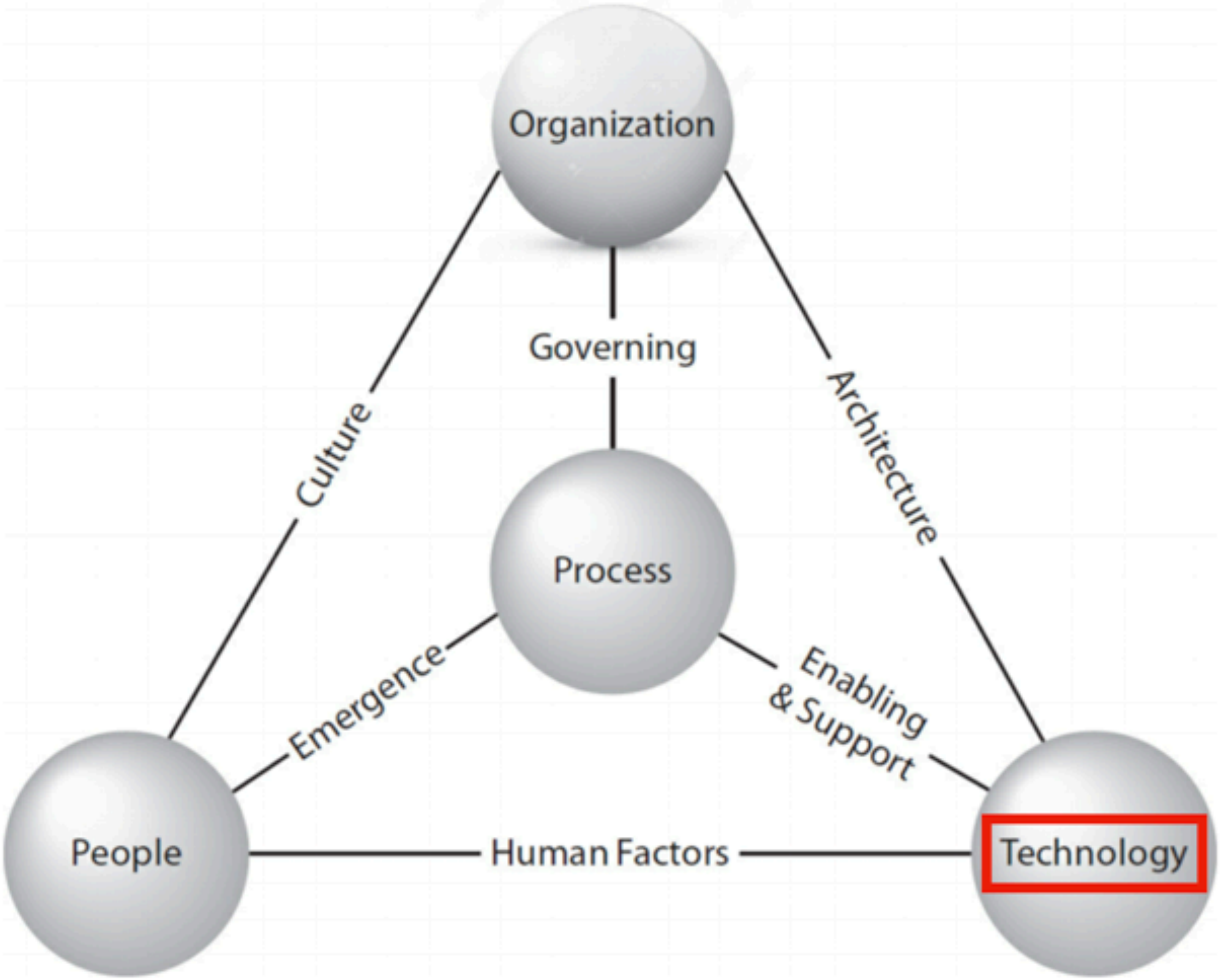


Example 2:
Causes for Process Weakness

- **An outside security audit shows that servers are months behind in security patches**
- **The company uses a vulnerability scanner to keep up-to date, for compliance**
- **Why is it failing?**

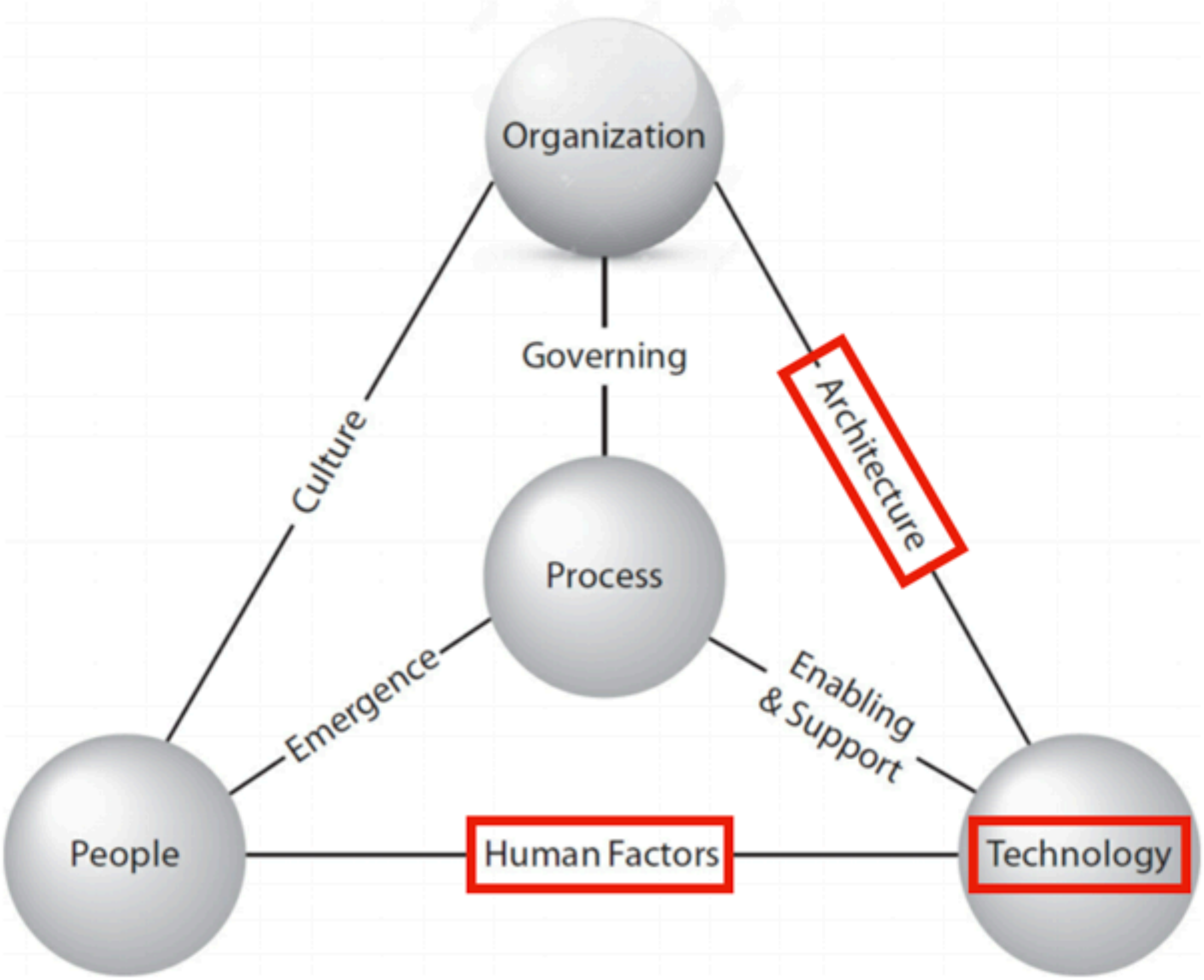
Example 2:
Causes for Process Weakness

- **Possible causes:**
  - **Technology -- scanner is faulty**



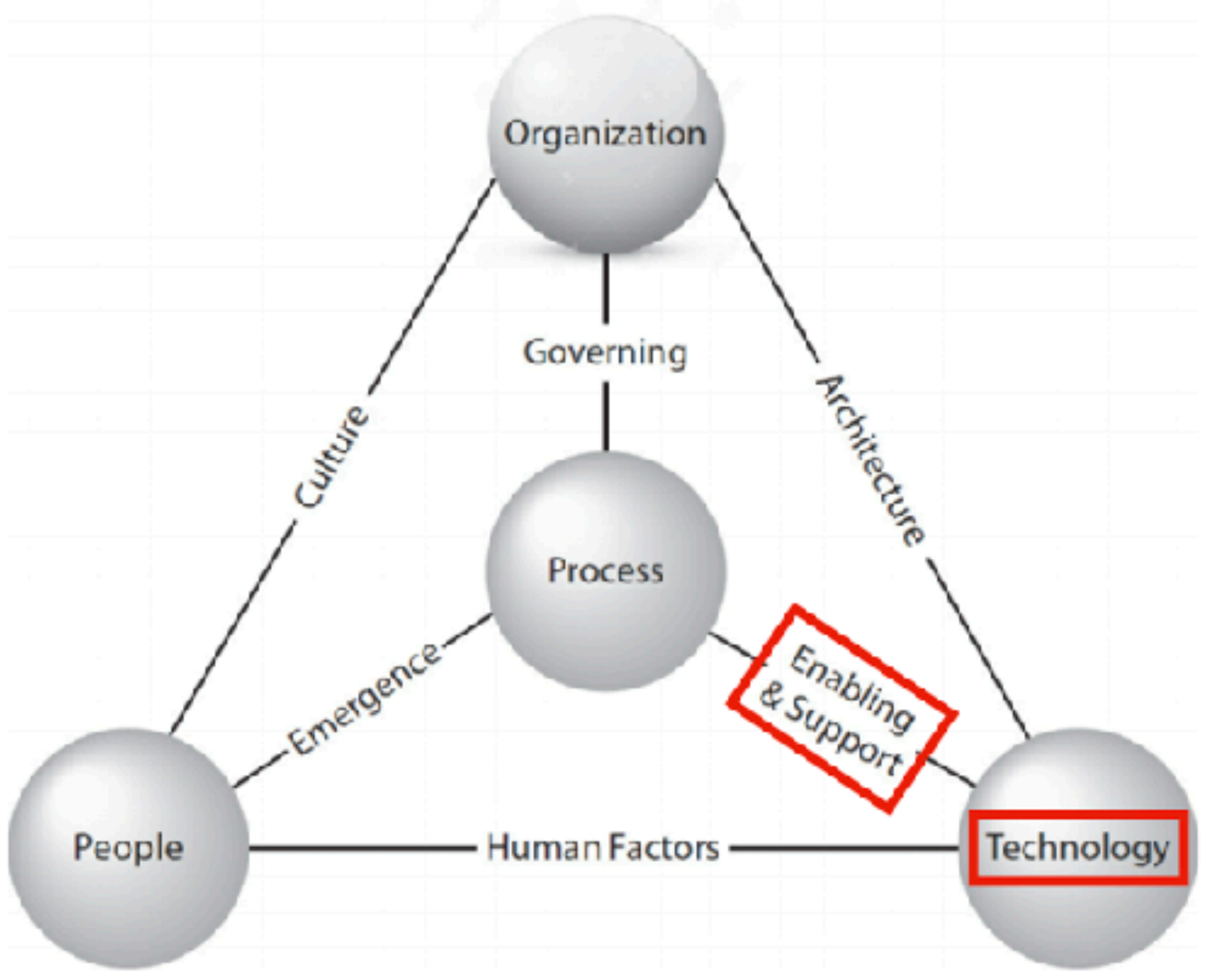
Example 2:
Causes for Process Weakness

- **Possible causes:**
  - **Architecture--scanner can't reach all systems in network**
  - **Human factors--engineers not using scanner properly**



Example 2: Causes for Process Weakness

- **Possible causes:**
  - **Enabling & Support--Interview engineers about business processes**
  - **New networks have been added that are not included in scanner's configuration**



Kahoot!

Ch 2a-1

Kahoot!