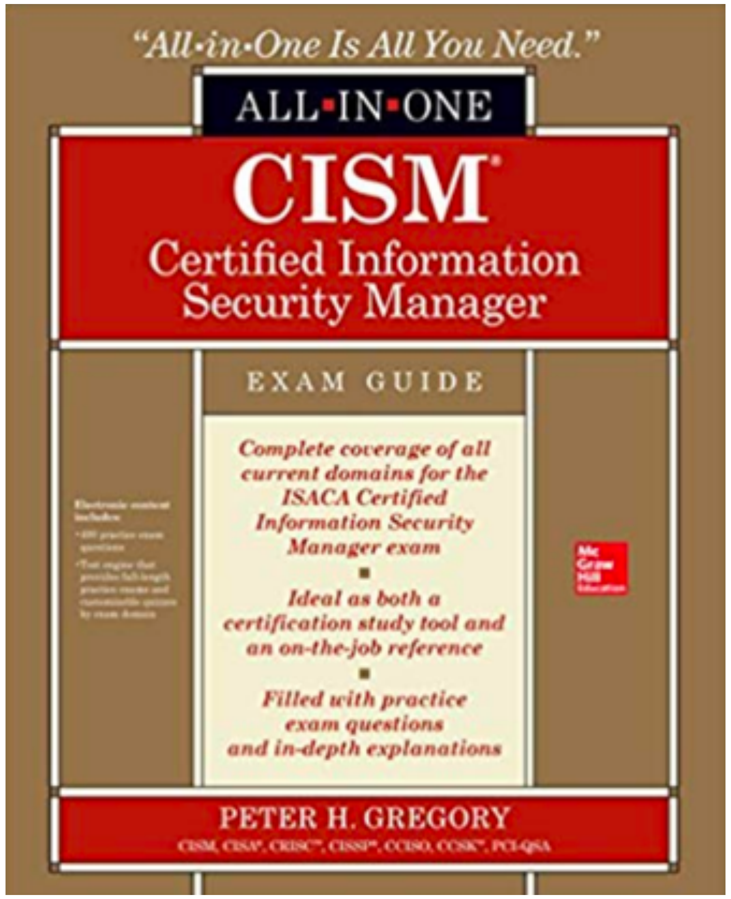
CNIT 160: Cybersecurity Responsibilities

3. Information Risk Management

Part 1

Pages 102 - 115


"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
CISM, CISA, CRISC, CISSP, CCISO, CCSK, PCI-QSA
Mc Graw Hill Education

Updated 2-10-22

Topics

- **Part 1 (p. 102 - 115)**
  - **Risk Management Concepts**
  - **Implementing a Risk Management Program**
- **Part 2 (p. 114 - 125)**
  - **The Risk Management Life Cycle**
    - **The Risk Management Process**
    - **Risk Management Methodologies**

Topics

- **Part 3 (p. 125 - 158)**
  - **The Risk Management Life Cycle**
    - **Starting at "Asset Identification and Valuation"**
- **Part 4 (p. 158 - 182)**
  - **Operational Risk Management**

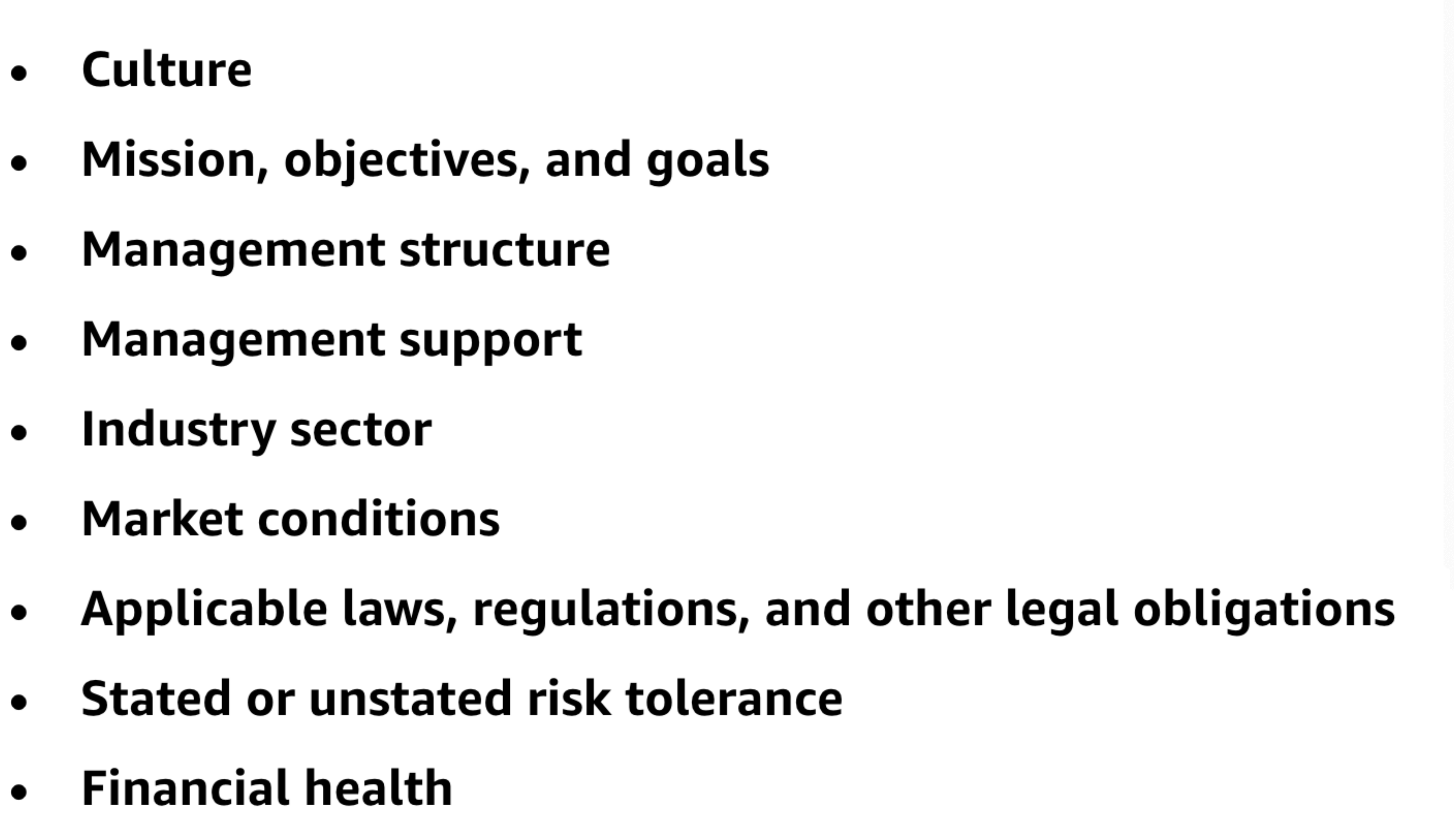
Risk Management

- **30% of the CISM exam**
- **The practice of balancing business opportunity with potential information security-related losses**
- **Largely qualitative**

Effectiveness

- Effectiveness of risk management depends on
  - Support from executive management
  - Organization's culture with respect to security awareness and accountability
- Each risk management program is different, depending on several factors

Factors

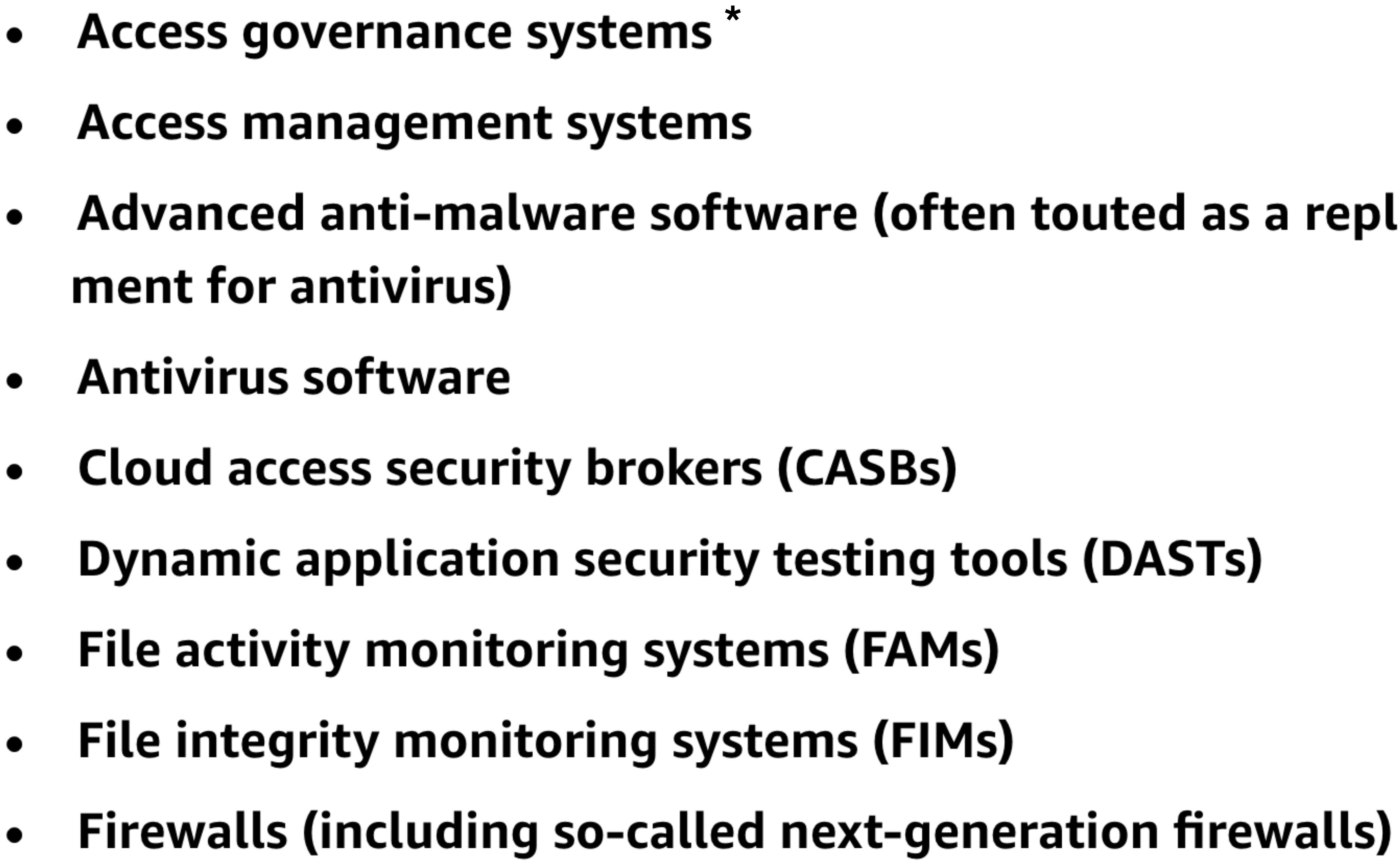


- **Culture**
- **Mission, objectives, and goals**
- **Management structure**
- **Management support**
- **Industry sector**
- **Market conditions**
- **Applicable laws, regulations, and other legal obligations**
- **Stated or unstated risk tolerance**
- **Financial health**

Outcomes of Risk Management

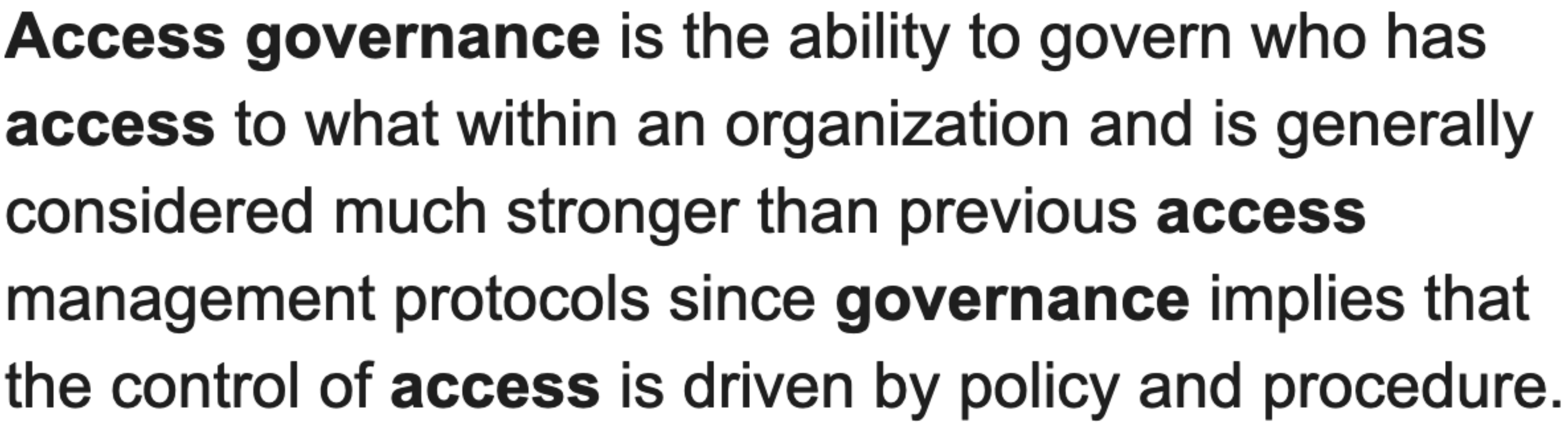
- **Greatest benefits**
  - **Lower probability of security incidents**
  - **Reduced impact from incidents**
- **Culture of risk-aware planning, thinking, and decision-making**

Technologies



- Access governance systems *
- Access management systems
- Advanced anti-malware software (often touted as a replacement for antivirus)
- Antivirus software
- Cloud access security brokers (CASBs)
- Dynamic application security testing tools (DASTs)
- File activity monitoring systems (FAMs)
- File integrity monitoring systems (FIMs)
- Firewalls (including so-called next-generation firewalls)

*** see next slide**



Access governance is the ability to govern who has **access** to what within an organization and is generally considered much stronger than previous **access** management protocols since **governance** implies that the control of **access** is driven by policy and procedure.

- **From cso.com**

Technologies

- Forensics tools
- Governance, risk, and compliance (GRC) systems *
- Intrusion detection systems (IDSs)
- Intrusion prevention systems (IPSs)
- Network access controls
- Phishing assessment
- Privileged access management systems (PAMs)
- Public key infrastructure (PKI)
- Security information and event management system (SIEM)
- Single sign-on (SSO) systems
- Static application security testing tools (SASTs)

* see next slide

GRC

- **"Governance, risk and compliance (GRC) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Think of GRC as a structured approach to aligning IT with business objectives, while effectively managing risk and meeting compliance requirements."**
  - **From cio.com**

Technologies

- **Spam filters**
- **Third-party risk management systems (TPRMs)**
- **User behavioral analytics systems (UBAs)** *
- **Unified threat management systems (UTMs)** *
- **Virtual private network (VPN) systems**
- **Vulnerability scanning tools**
- **Web application scanning tools**
- **Web filtering**
- **Wireless access controls**
- **External monitoring and intelligence services**

*** see following slides**

UBA

- "a cybersecurity process about detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats."
  - From Wikpiedia.org

What is unified threat management?

Originally called unified threat management (UTM), these capabilities better known as a Next-Generation Firewall (NGFW) today, provide multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. NGFW includes functions such as anti-virus, anti-spam, content filtering, and web filtering.

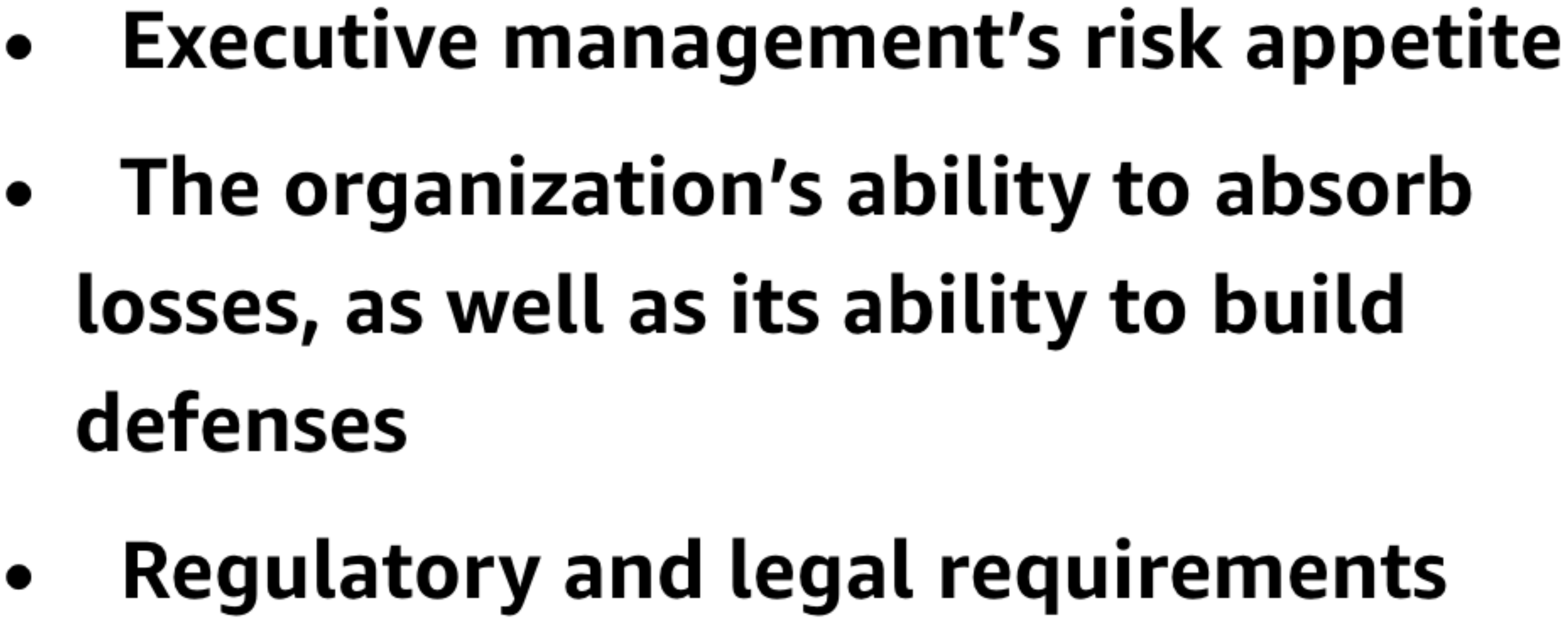
Kahoot!

Ch 3a-1

Purchasing Decisions

- **With risk management:**
  - **Identify specific risks**
  - **Choose to mitigate those risks with specific solutions**
- **Without risk management, choices come from**
  - **Salespeople**
  - **Imitating other companies**
  - **Articles in trade publications**

Risk Tolerance Factors



- Executive management's risk appetite
- The organization's ability to absorb losses, as well as its ability to build defenses
- Regulatory and legal requirements

- **Risk assessments and risk treatments drive adjustments to controls**

Relationships

- **IT and security can't be the "no" group**
- **Become a business enabler**
- **Role: security catalyst**

Communication

- Stakeholders need to understand
  - How risk management works
  - What role they will play in it to achieve business objectives
  - Impact on relationships and autonomy
  - How the program will improve the organization, including their own jobs
- Be as transparent as possible
  - Some items are still confidential

Security Awareness

- Given to entire organization
- Basics of security

The Leader in Security Awareness Training
KEVIN MITNICK
Security Awareness Training

Risk Awareness

- Given to senior personnel
- Ensures that they know
  - All business decisions have implications on information risk
  - Presence of a formal risk management program
  - Process and techniques for making risk-aware decisions

Risk Consulting

- Security managers often act as consultants within their organization
- Requires relationships of trust
- Treat these mini-consulting engagements as formal service requests
- Be responsive

Information Risk Consultant

- **Key attributes**
  - **Ability to listen to business leaders**
  - **Ability to assess impact on a process or business unit, and identify other areas of the business the issue may cascade to**
  - **Understand business, not just technology**

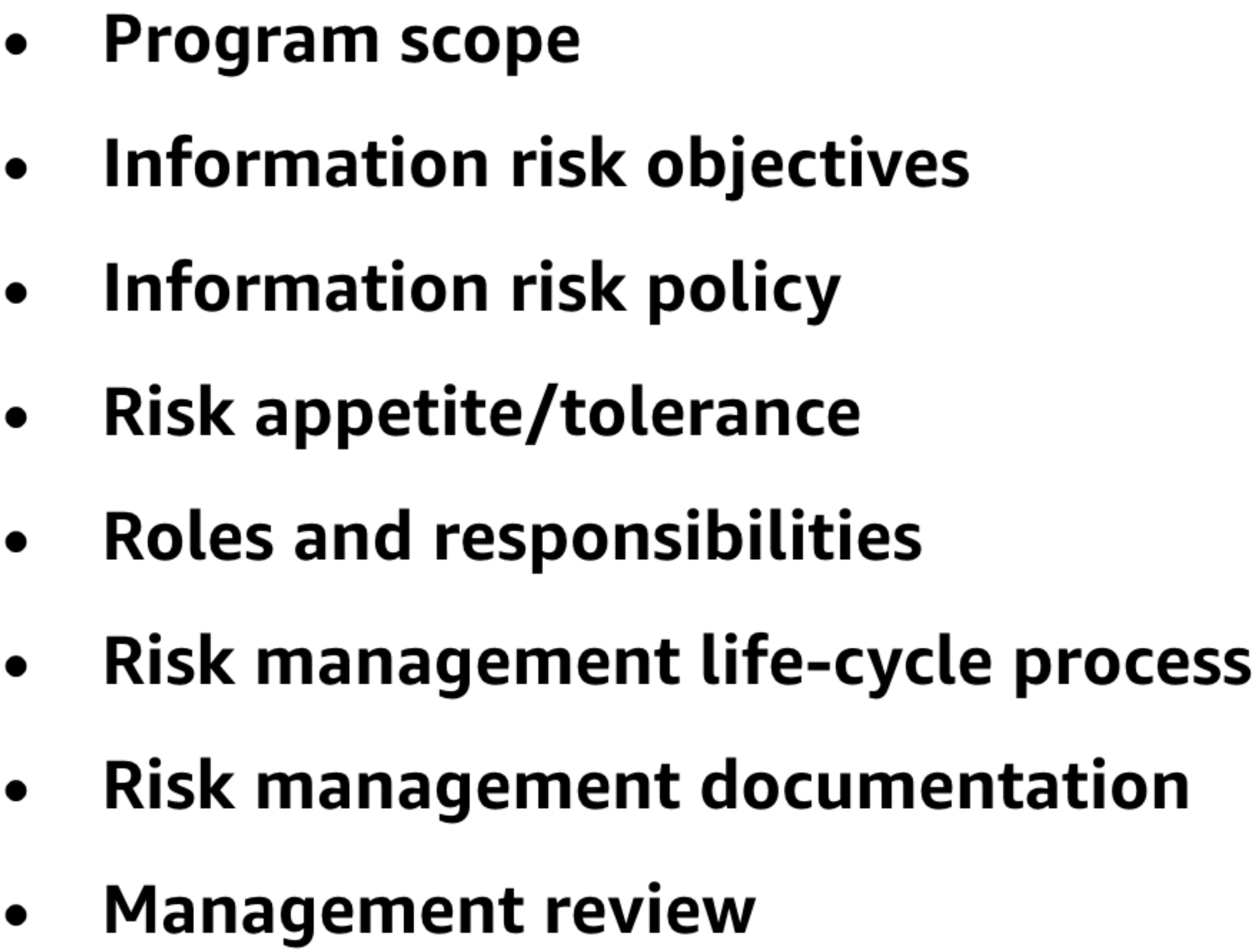
Risk Management Frameworks

- ISO/IEC 27001, “Information technology — Security techniques — Information security management systems — Requirements.” Requirements 4 through 10 in this standard describe the structure of an entire information security management system (ISMS) including risk management.
- ISO/IEC 27005, “Information Technology — Security Techniques — Information security risk management.”
- ISO/IEC 31010, “Risk management — Risk assessment techniques.”

Risk Management Frameworks

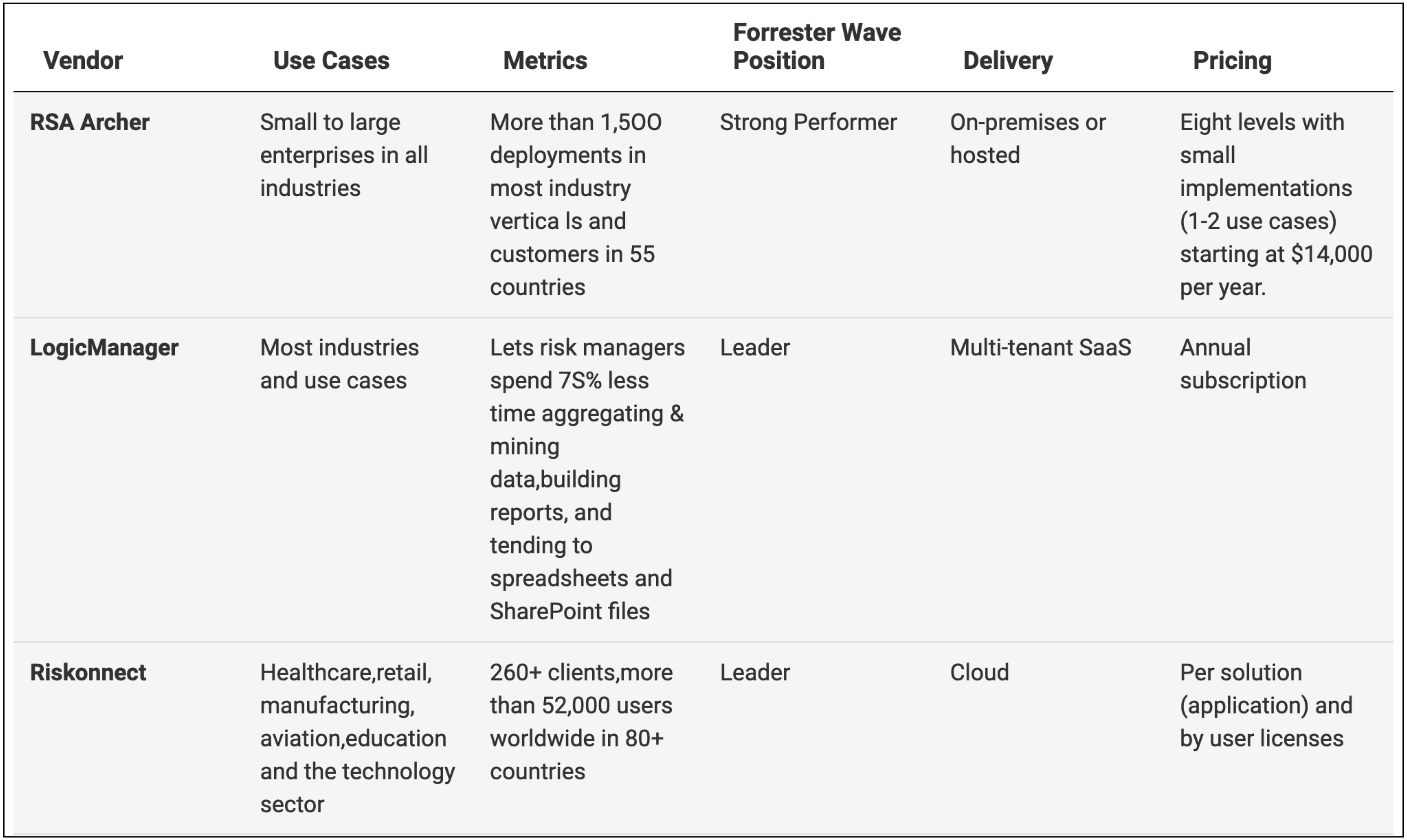
- **NIST Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.”**
- **NIST Special Publication 800-39, “Managing Information Security Risk.”**
- **COBIT 5.**
- **RIMS Risk Maturity Model.**
- **Facilitated Risk Assessment Process.**

Framework Components



- Program scope
- Information risk objectives
- Information risk policy
- Risk appetite/tolerance
- Roles and responsibilities
- Risk management life-cycle process
- Risk management documentation
- Management review

Governance, Risk, and Compliance (GRC) Systems



Vendor	Use Cases	Metrics	Forrester Wave Position	Delivery	Pricing
RSA Archer	Small to large enterprises in all industries	More than 1,5OO deployments in most industry vertica ls and customers in 55 countries	Strong Performer	On-premises or hosted	Eight levels with small implementations (1-2 use cases) starting at $14,000 per year.
LogicManager	Most industries and use cases	Lets risk managers spend 7S% less time aggregating & mining data,building reports, and tending to spreadsheets and SharePoint files	Leader	Multi-tenant SaaS	Annual subscription
Riskonnect	Healthcare,retail, manufacturing, aviation,education and the technology sector	260+ clients,more than 52,000 users worldwide in 80+ countries	Leader	Cloud	Per solution (application) and by user licenses

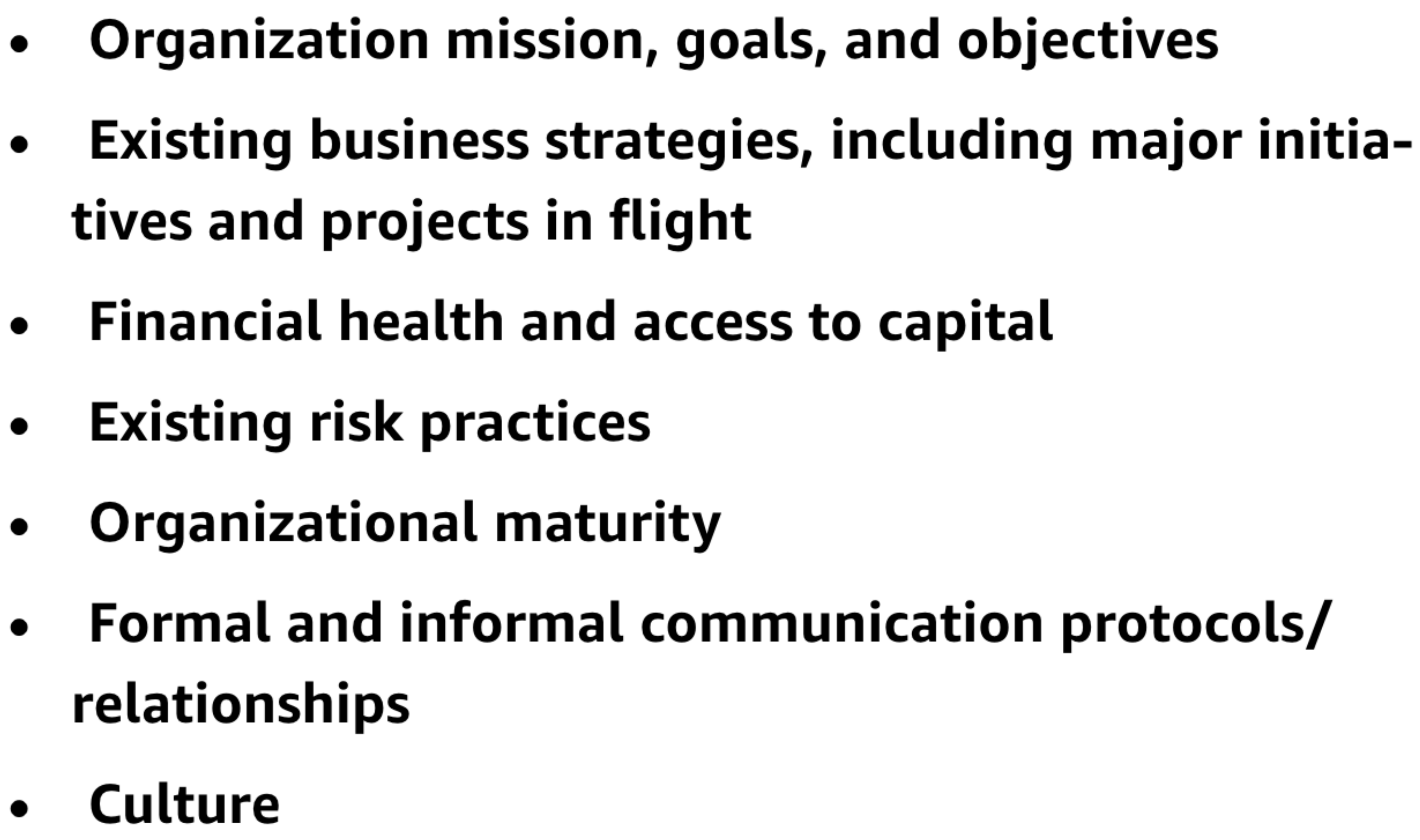
Integration into the Environment

- **Use a GRC platform to manage policies and external vendors**
- **To minimize disruption to the organization**
- **Integrating into culture is the most important consideration**

Risk Management Context

- **Risk management program may operate only within part of the business**
- **Or the entire organization**

Internal Environments



- Organization mission, goals, and objectives
- Existing business strategies, including major initiatives and projects in flight
- Financial health and access to capital
- Existing risk practices
- Organizational maturity
- Formal and informal communication protocols/ relationships
- Culture

External Environments

- **Market conditions**
- **Economic conditions**
- **Applicable laws and regulations**
- **Social and political environments**
- **External stakeholders including regulators, business partners, suppliers, and customers**
- **External threats and threat actors**
- **Geopolitical factors**

Gap Analyses

- **Examination of process or system**
  - **To determine differences between**
    - **Existing state, and**
    - **Desired future state**

Example of Gap Analysis

- **Change control process**
  - **Currently: only a log of changes and emails containing management approval**
  - **Lacking:**
    - **Change request procedure**
    - **Change Advisory Board (CAB)**
    - **Roles and responsibilities**
    - **More fields and annotations in the log**

External Support

- **Every security manager is lacking in some areas**
  - **Experience with risk management programs**
  - **Experience in this security sector**
  - **Familiarity with tools, technologies, or processes**

Information Sources

- **Security round tables**
- **Organization chapters**
  - **ISSA, $(ISC)^2$, ISACA**
  - **Society for Information Management (SIM)**
  - **Society of Information Risk Analysts (SIRA)**
  - **Cloud Security Alliance (CSA)**
  - **InfraGard**
  - **International Association of Privacy Professionals (IAPP)**

Information Sources

- Published risk management practices
  - From (ISC)^2, ISACA, SANS
- Security Industry News
  - Information Security, SC, CSO Magazines
  - Dark Reading
  - TechTarget
  - (ISC)^2, ISACA, SANS

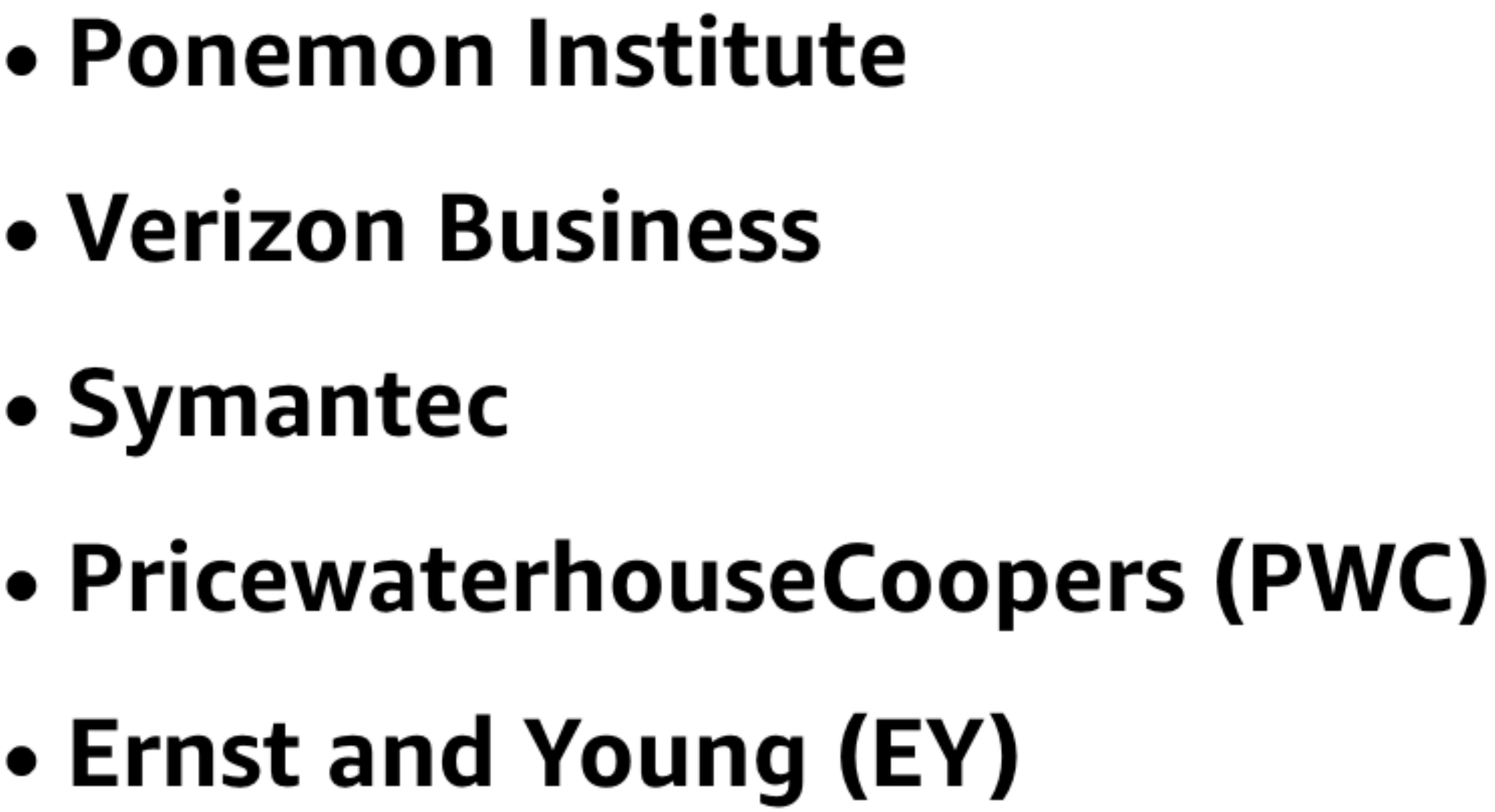
RISKY.BIZ
It's a jungle out there

Paul's Security Weekly

Paul's Security Weekly

Information Sources

- **Reports from research organizations**



  - **Ponemon Institute**
  - **Verizon Business**
  - **Symantec**
  - **PricewaterhouseCoopers (PWC)**
  - **Ernst and Young (EY)**

Information Sources

- **Advisory services**

  - Gartner
  - Forrester
  - IDC
  - Ovum
  - Frost Sullivan

Information Sources

- **Consulting firms**
- **Training**
- **Books**

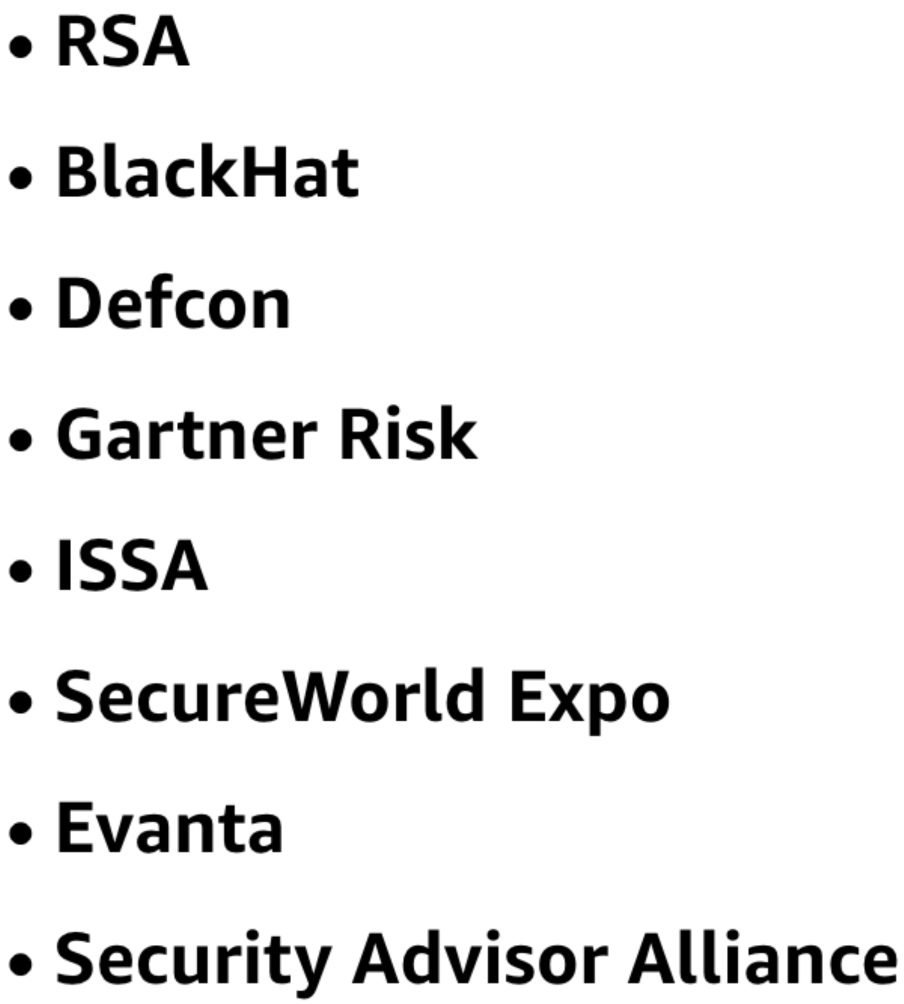
https://cybercanon.paloaltonetworks.com

CYBERSECURITY CANON

ZERO DAY THREAT
BYRON ACOHIDO AND JON SWARTZ
BRUCE SCHNEIER
CLICK HERE TO KILL EVERYBODY
Security and Survival in a Hyper-connected World
DIGITAL RESILIENCE
Is Your Company Ready for the Next Cyber Threat?
RAY A. ROTHROCK
CYBERSECURITY
A BUSINESS SOLUTION
HACKS THAT SHOCKED THE BUSINESS WORLD
CYBER WARS
CHARLES ARTHUR
WILEY
Security Engineering
Ross Anderson
SECOND EDITION
ENGINEERING TRUSTWORTHY SYSTEMS
READ MORE
DISRUPT OR DIE
JEDIDIAH YUEH
O'REILLY
Zero Trust Networks
Evan Gilman & Doug Barth
SMALL BUSINESS CYBER SECURITY
YOUR CUSTOMERS CAN TRUST YOU...RIGHT?
Dr. Erdal Ozkaya
Learn Social Engineering
Packt
NATIONAL BESTSELLER
The Shadow Factory
JAMES BAMFORD
The Ultra-Secret NSA from 9/11 to the Eavesdropping on America
O'REILLY
Chaos Engineering
Building Confidence in System Behavior through Experiments
NO MORE MAGIC WANDS
TRANSFORMATIVE CYBERSECURITY CHANGE FOR EVERYONE
BY GEORGE FINNEY, J.D., CISO
NEW YORK TIMES BESTSELLER
Abundance
THE FUTURE IS BETTER THAN YOU THINK
CYBERSECURITY
A BUSINESS SOLUTION
EXPONENTIAL ORGANIZATIONS
SALIM ISMAIL
Winner!
crypto
STEVEN LEVY
CISO DESK REFERENCE GUIDE
Bill Bonney · Gary Hayslip · Matt Stamper
AMERICAN KINGPIN
NICK BILTON
Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig

Information Sources

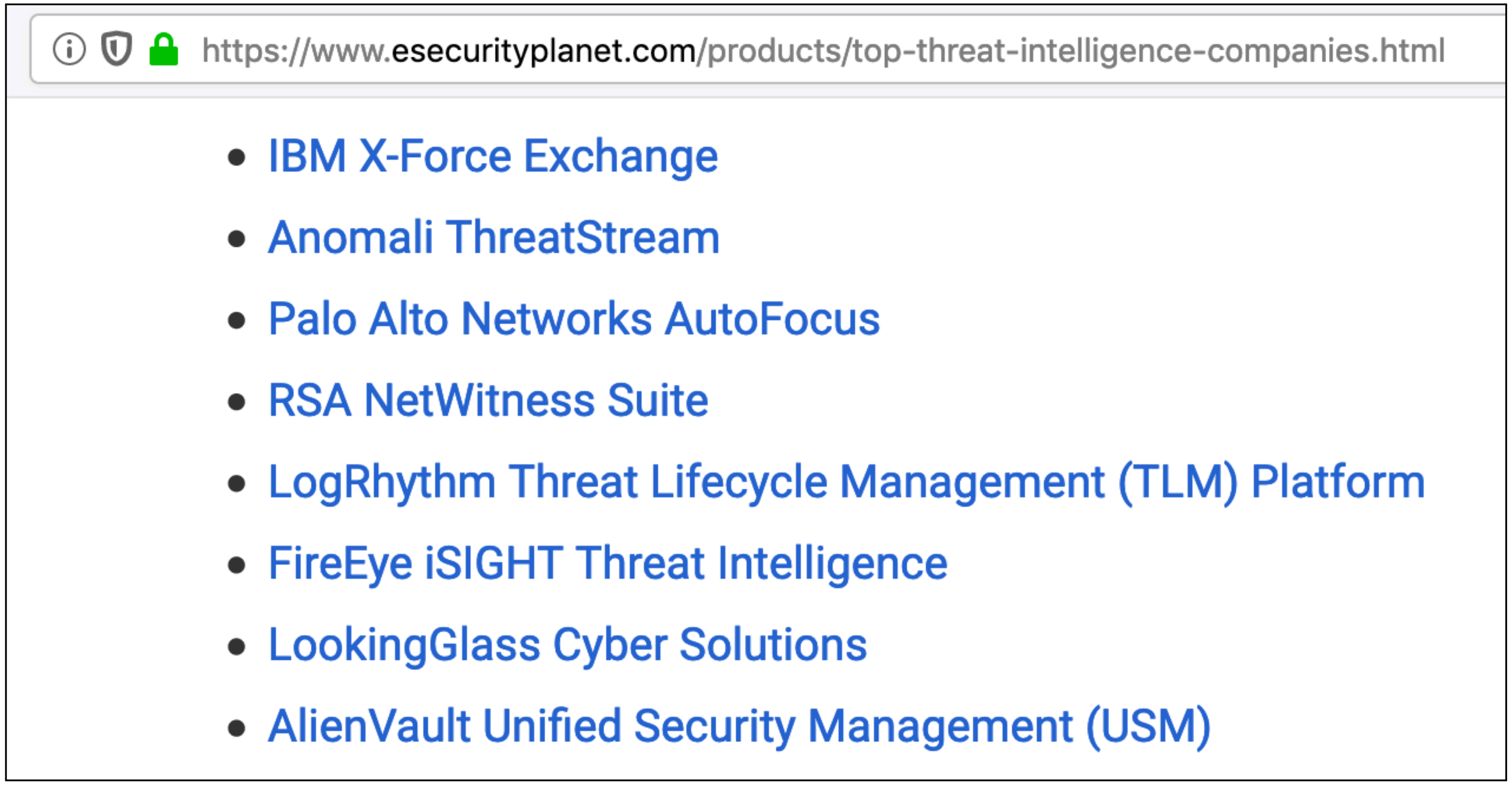
- **Conferences**



  - **RSA**
  - **BlackHat**
  - **Defcon**
  - **Gartner Risk**
  - **ISSA**
  - **SecureWorld Expo**
  - **Evanta**
  - **Security Advisor Alliance**

Information Sources

- Security Intelligence Services
- Human-readable, or machine-readable for import into SIEM



https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html

- IBM X-Force Exchange
- Anomali ThreatStream
- Palo Alto Networks AutoFocus
- RSA NetWitness Suite
- LogRhythm Threat Lifecycle Management (TLM) Platform
- FireEye iSIGHT Threat Intelligence
- LookingGlass Cyber Solutions
- AlienVault Unified Security Management (USM)

Kahoot!

Ch 3a-2