CYBER 503x
Cybersecurity Risk Management

Unit 5: Security Metrics 2

Re-cap: Security Metrics Type (1)
- Defining Technical Diagnostic Metrics

- Technical metrics:
  - Perimeter defenses
  - Coverage and control
  - Availability and reliability
  - Application risks
    - Defect counts, cyclomatic complexity, and application risk indices help quantify the risks inherent to homegrown code and 3rd party software.

Application Security

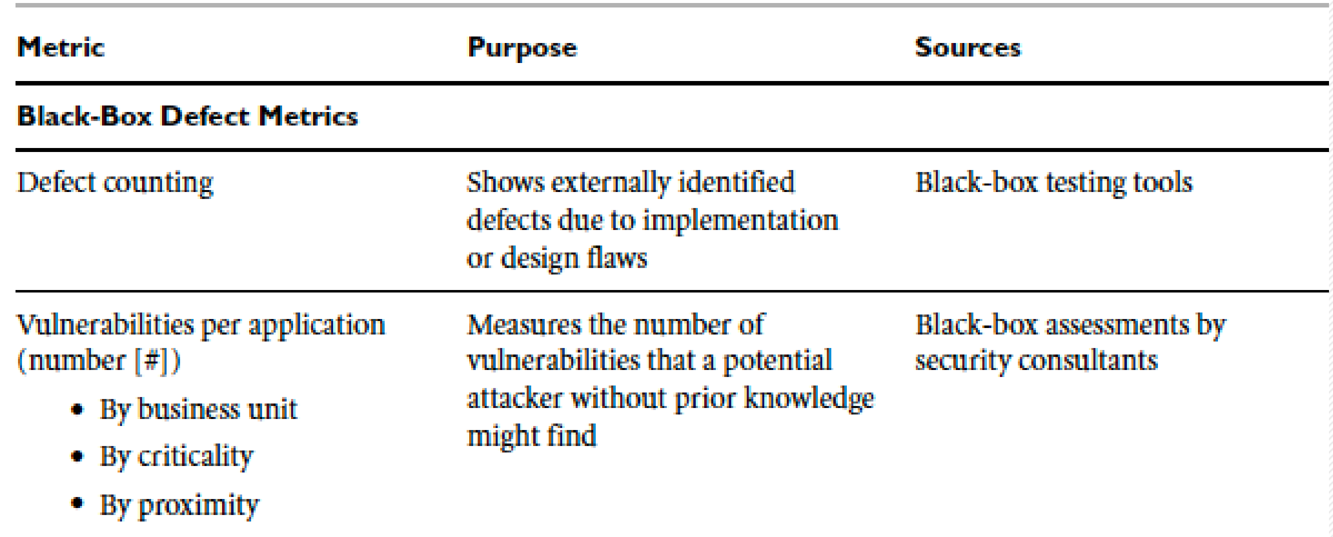
- Applications are the electronic engines that drive most business. For instance, e-commerce applications, order processing and management software, supply chain management, the ERP (Enterprise Resource Planning) systems, etc.
  - In-house developed
  - Packaged
  - Outsourced
  - Served on demand
- Gartner Group stated that 75% of attacks tunneled through or used application related threat vectors.
- It represents an entirely separate measurement domain with its own diagnostics.

Three ways to measure application security

- Black-Box Defect Metrics
- Qualitative process metrics and indices
- Code security metrics

Black-Box Defect Metrics

- SQL injection
- Command injection
- Parameter tampering
- Cross-site scripting
- Buffer overflows



Metric	**Purpose**	**Sources**
Black-Box Defect Metrics		
Defect counting	Shows externally identified defects due to implementation or design flaws	Black-box testing tools
Vulnerabilities per application (number [#]) • By business unit • By criticality • By proximity	Measures the number of vulnerabilities that a potential attacker without prior knowledge might find	Black-box assessments by security consultants

Qualitative process metrics and indices

- Application development lifecycle
  - Design reviews: at the midpoint of the design stage
    - Validation of security engineering principles
    - Identifies gaps compared to security standards
  - Architecture assessment: at the midpoint of development
    - Verification of implemented security standards
    - Finds potential architectural weakness
  - Code reviews (optional): at the end of development for sensitive functions
    - Focused examination of sensitive functions
    - Find development flaws
  - Penetration test: prior to deployment
    - Identification of deployment flaws
    - Finds “real-world” vulnerabilities

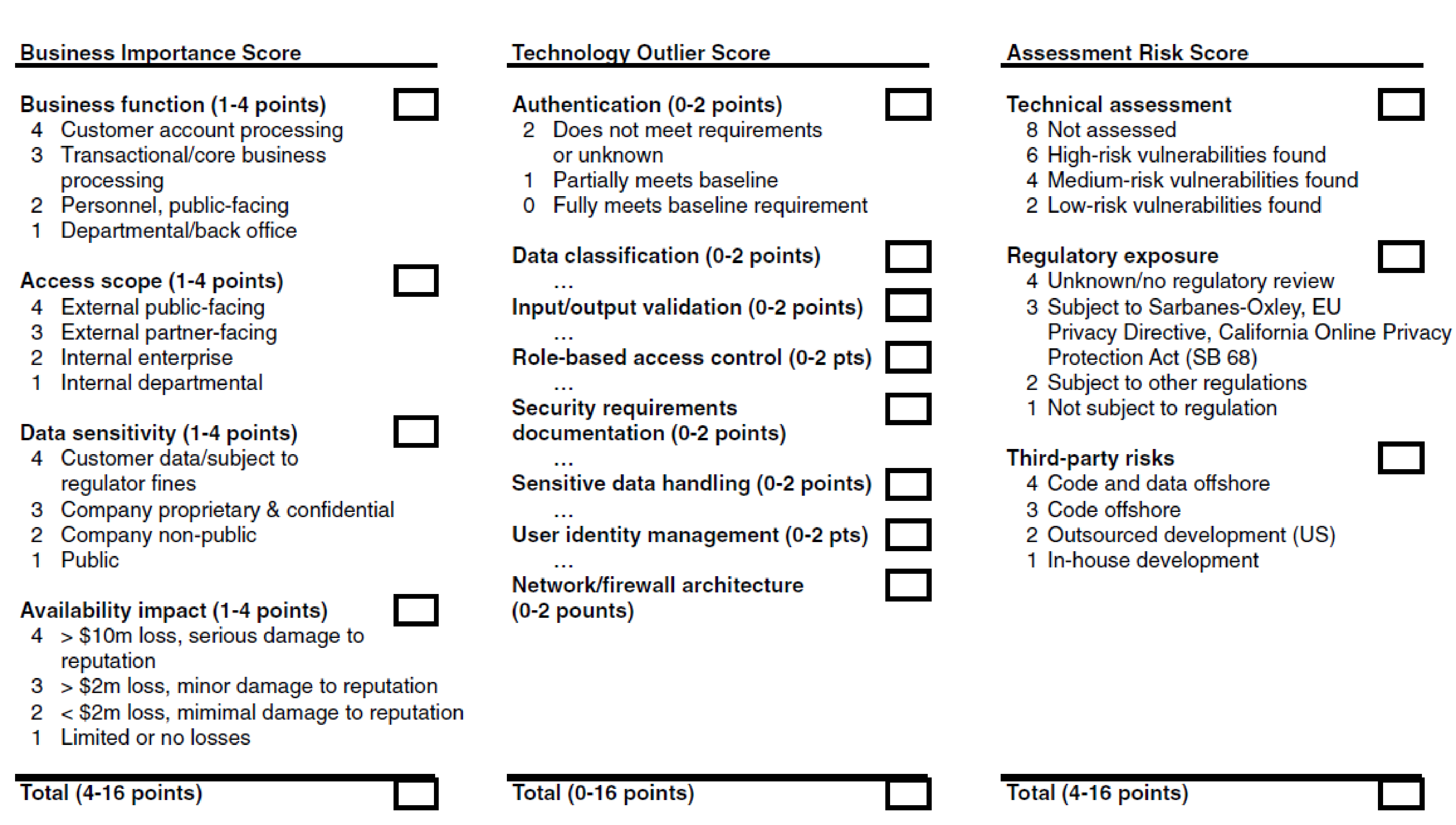
Business-Adjusted Risk (BAR)

- BAR (1 to 25) =
  business impact (1 to 5) x
  risk of exploit (1 to 5, depending on business context)
  - Risk of exploit: how easily an attacker can exploit a given defect (5: high risk, easiest to exploit)
  - Business impact: the damage that would be sustained if the defect were exploited. (5: significant impact)
  - The higher the BAR score, the higher the risk
  - Similar to ALE = SLE x ORA

Application Insecurity Index

- A sample scoring technique that focuses on factual questions – Application Insecurity Index (AII)
    - Fact-based questions that result in binary yes/no answers serve as the basis of the score.

Application Insecurity Index



Business Importance Score

Business function (1-4 points) □
4 Customer account processing
3 Transactional/core business processing
2 Personnel, public-facing
1 Departmental/back office

Access scope (1-4 points) □
4 External public-facing
3 External partner-facing
2 Internal enterprise
1 Internal departmental

Data sensitivity (1-4 points) □
4 Customer data/subject to regulator fines
3 Company proprietary & confidential
2 Company non-public
1 Public

Availability impact (1-4 points) □
4 > $10m loss, serious damage to reputation
3 > $2m loss, minor damage to reputation
2 < $2m loss, mimimal damage to reputation
1 Limited or no losses

Total (4-16 points) □

Technology Outlier Score

Authentication (0-2 points) □
2 Does not meet requirements or unknown
1 Partially meets baseline
0 Fully meets baseline requirement

Data classification (0-2 points) □
...

Input/output validation (0-2 points) □
...

Role-based access control (0-2 pts) □
...

Security requirements documentation (0-2 points) □
...

Sensitive data handling (0-2 points) □
...

User identity management (0-2 pts) □
...

Network/firewall architecture (0-2 pounts) □

Total (0-16 points) □

Assessment Risk Score

Technical assessment □
8 Not assessed
6 High-risk vulnerabilities found
4 Medium-risk vulnerabilities found
2 Low-risk vulnerabilities found

Regulatory exposure □
4 Unknown/no regulatory review
3 Subject to Sarbanes-Oxley, EU Privacy Directive, California Online Privacy Protection Act (SB 68)
2 Subject to other regulations
1 Not subject to regulation

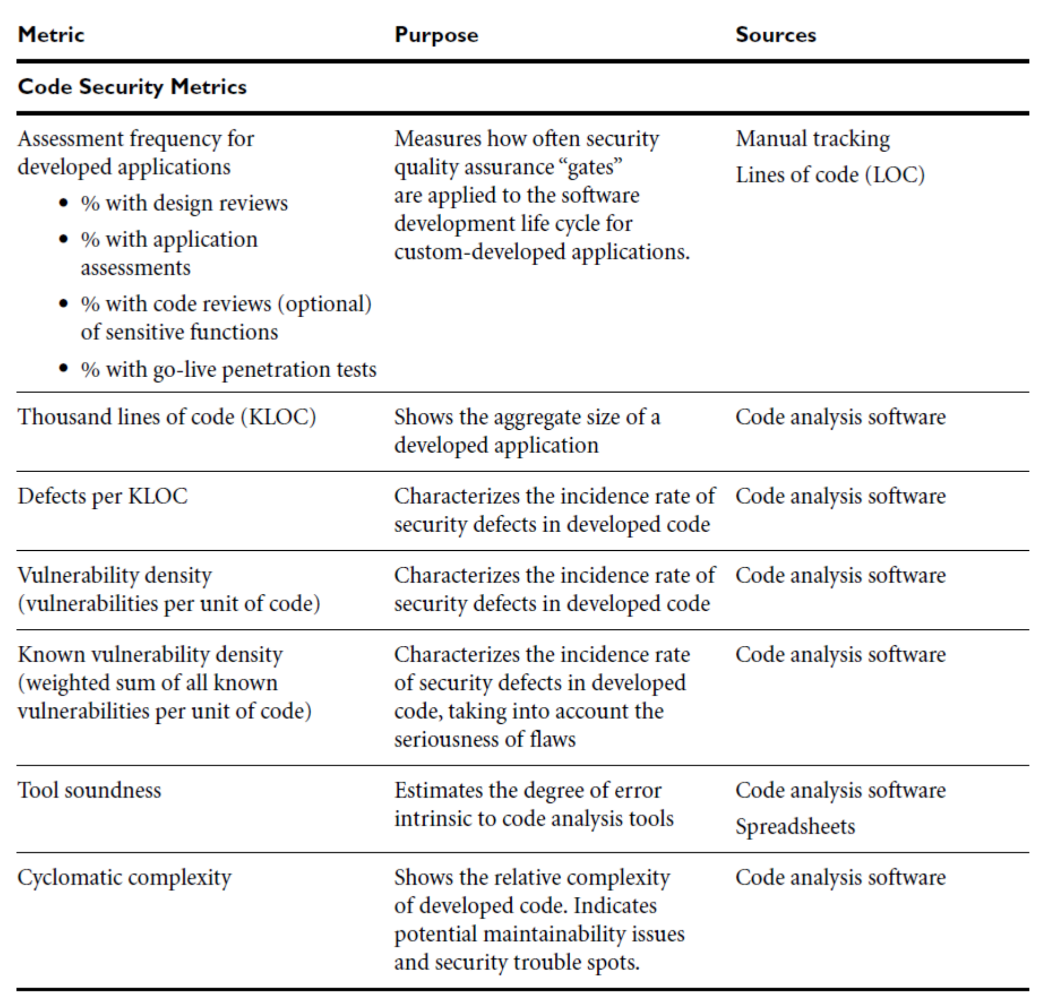
Third-party risks □
4 Code and data offshore
3 Code offshore
2 Outsourced development (US)
1 In-house development

Total (4-16 points) □

Code Security Metrics

- They tackle measurement of software quality directly.
  - “code volume”: LOC, KLOC
    - Not directly related to security, but provide texture, depth and context.
  - “use case points” (more subjective)
    - Suffer from methodological inconsistencies and relatively difficult to count them.
  - “security defects”: a flaw in the code as detected by automated code-scanning programs (RATS, ITS4, Klocwork, Coverity, etc.)
    - Unsafe memory handling, lack of validation of user inputs, dead code blocks.

Code Security Metrics



Metric	Purpose	Sources
Code Security Metrics		
Assessment frequency for developed applications • % with design reviews • % with application assessments • % with code reviews (optional) of sensitive functions • % with go-live penetration tests	Measures how often security quality assurance "gates" are applied to the software development life cycle for custom-developed applications.	Manual tracking Lines of code (LOC)
Thousand lines of code (KLOC)	Shows the aggregate size of a developed application	Code analysis software
Defects per KLOC	Characterizes the incidence rate of security defects in developed code	Code analysis software
Vulnerability density (vulnerabilities per unit of code)	Characterizes the incidence rate of security defects in developed code	Code analysis software
Known vulnerability density (weighted sum of all known vulnerabilities per unit of code)	Characterizes the incidence rate of security defects in developed code, taking into account the seriousness of flaws	Code analysis software
Tool soundness	Estimates the degree of error intrinsic to code analysis tools	Code analysis software Spreadsheets
Cyclomatic complexity	Shows the relative complexity of developed code. Indicates potential maintainability issues and security trouble spots.	Code analysis software

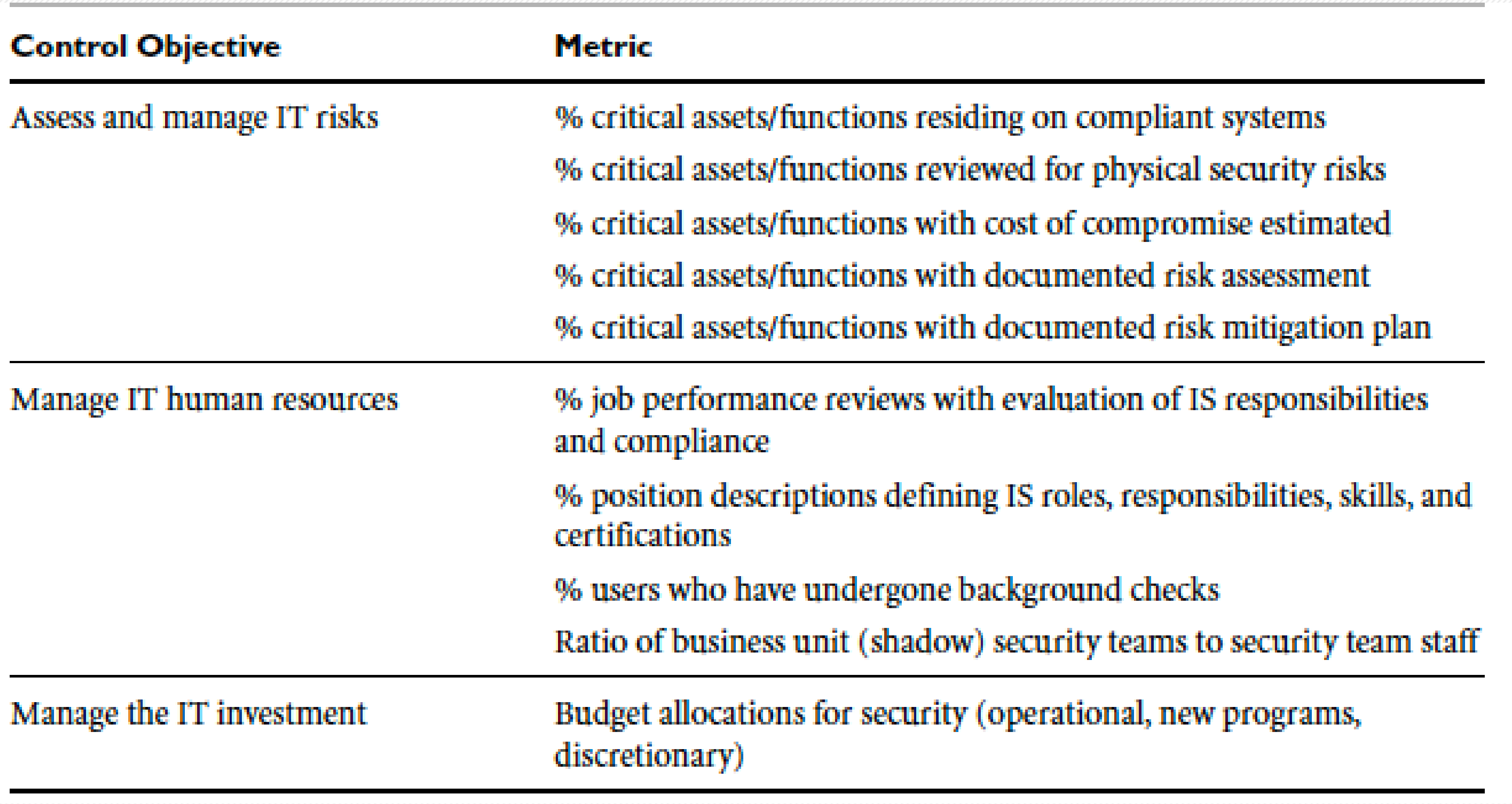
Security Program Elements

- Technology
- People
- Process

Measuring Program Effectiveness in 4 Domains - Use COBIT Framework

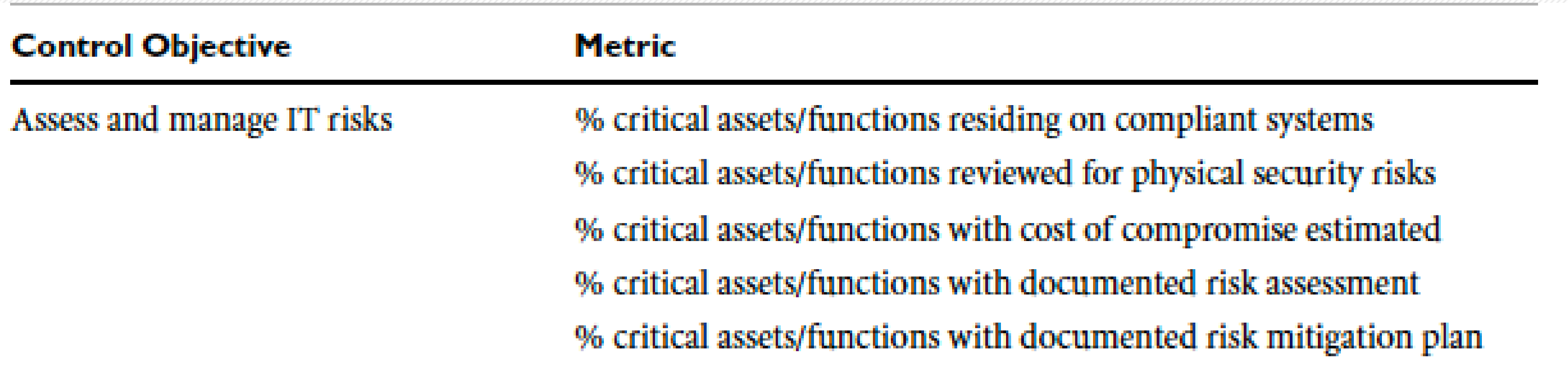
- Planning and organization
- Acquisition and implementation
- Delivery and support
- Monitoring

Planning and Organization Metrics



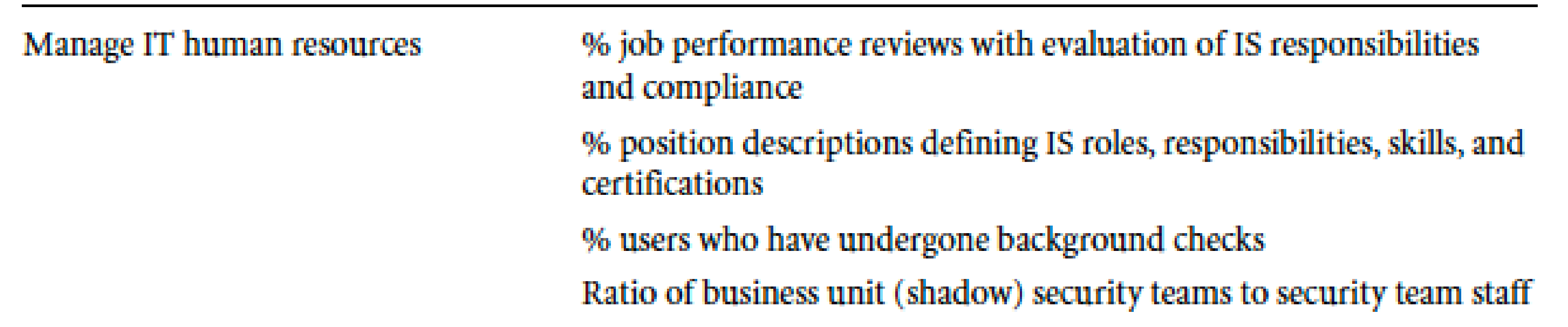
Control Objective	Metric
Assess and manage IT risks	% critical assets/functions residing on compliant systems
	% critical assets/functions reviewed for physical security risks
	% critical assets/functions with cost of compromise estimated
	% critical assets/functions with documented risk assessment
	% critical assets/functions with documented risk mitigation plan
Manage IT human resources	% job performance reviews with evaluation of IS responsibilities and compliance
	% position descriptions defining IS roles, responsibilities, skills, and certifications
	% users who have undergone background checks
	Ratio of business unit (shadow) security teams to security team staff
Manage the IT investment	Budget allocations for security (operational, new programs, discretionary)

Assessing Risk



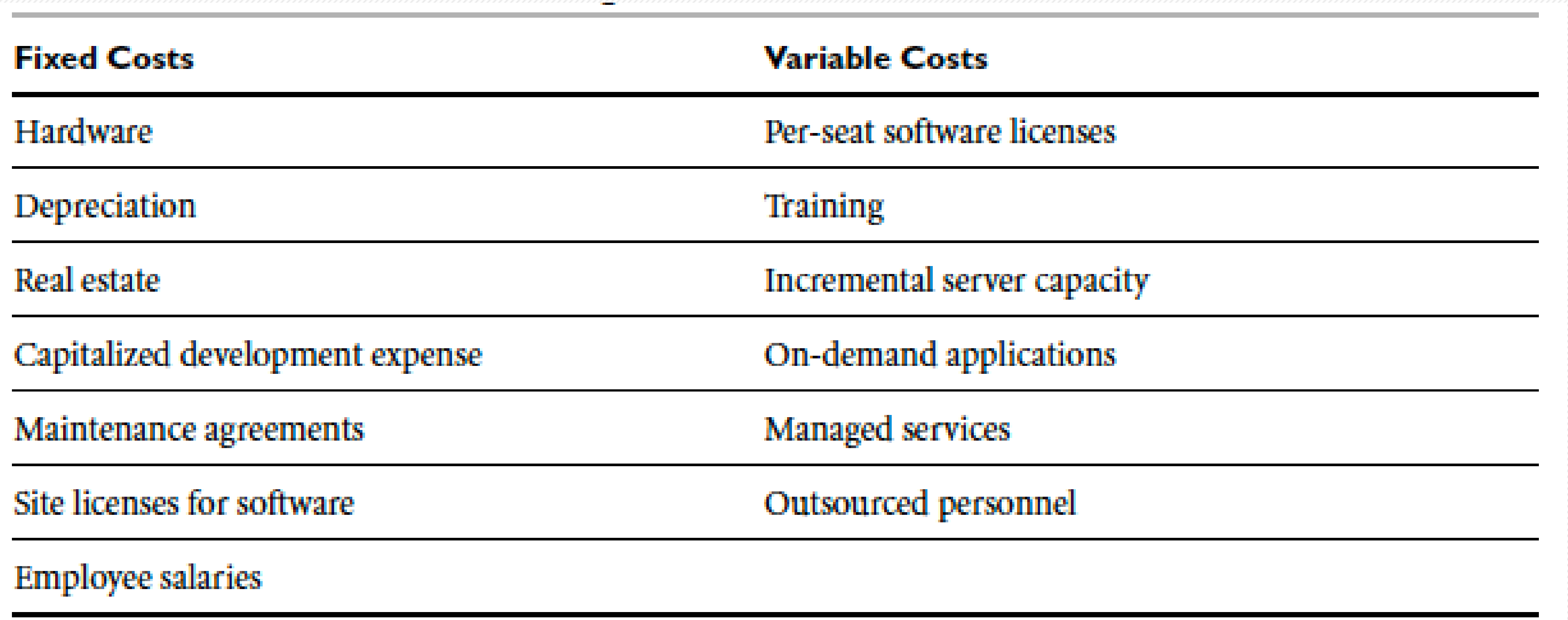
Control Objective	Metric
Assess and manage IT risks	% critical assets/functions residing on compliant systems
	% critical assets/functions reviewed for physical security risks
	% critical assets/functions with cost of compromise estimated
	% critical assets/functions with documented risk assessment
	% critical assets/functions with documented risk mitigation plan

Human Resources

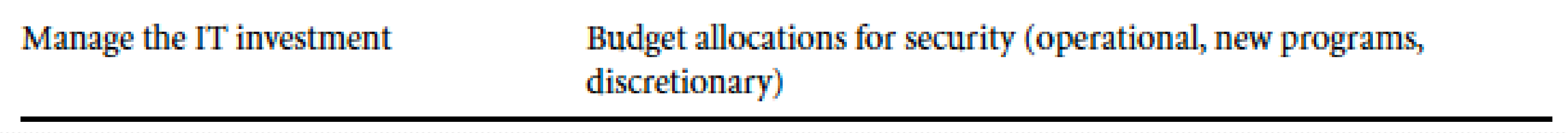


Manage IT human resources	% job performance reviews with evaluation of IS responsibilities and compliance
	% position descriptions defining IS roles, responsibilities, skills, and certifications
	% users who have undergone background checks
	Ratio of business unit (shadow) security teams to security team staff

Managing Investment



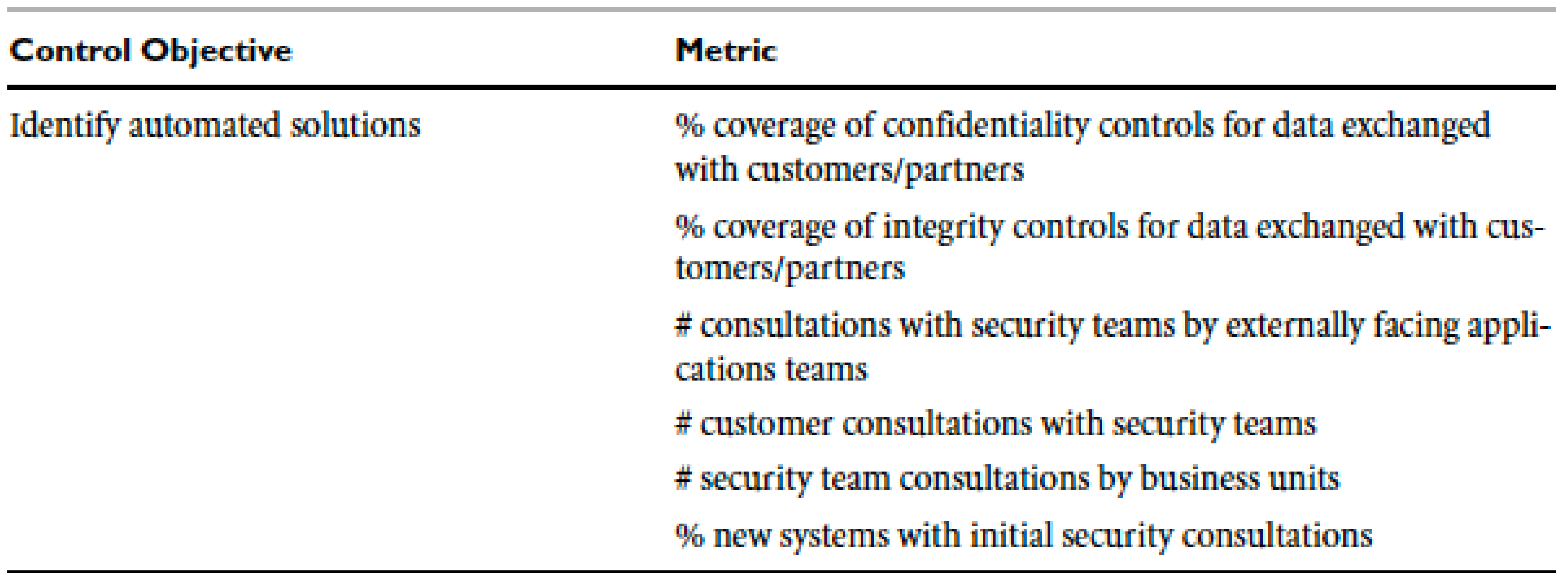
Fixed Costs	Variable Costs
Hardware	Per-seat software licenses
Depreciation	Training
Real estate	Incremental server capacity
Capitalized development expense	On-demand applications
Maintenance agreements	Managed services
Site licenses for software	Outsourced personnel
Employee salaries	



Manage the IT investment	Budget allocations for security (operational, new programs, discretionary)

Acquisition and Implementation (1)

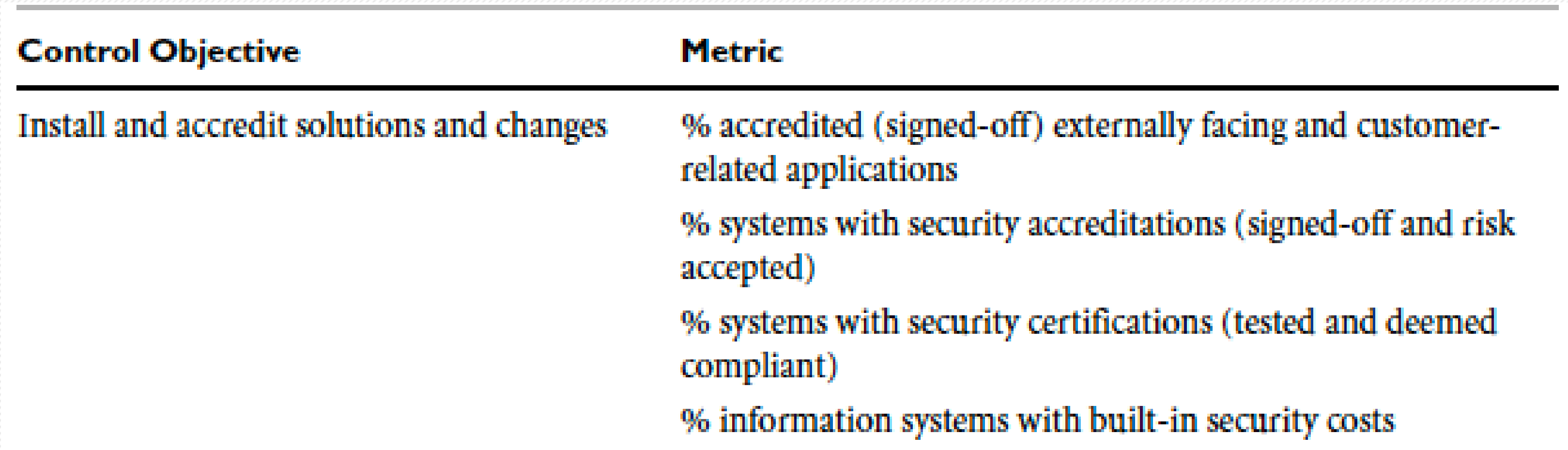
- Identifying Solutions



Control Objective	Metric
Identify automated solutions	% coverage of confidentiality controls for data exchanged with customers/partners % coverage of integrity controls for data exchanged with customers/partners # consultations with security teams by externally facing applications teams # customer consultations with security teams # security team consultations by business units % new systems with initial security consultations

Acquisition and Implementation (2)

- Installing and accrediting solutions



Control Objective	Metric
Install and accredit solutions and changes	% accredited (signed-off) externally facing and customer-related applications
	% systems with security accreditations (signed-off and risk accepted)
	% systems with security certifications (tested and deemed compliant)
	% information systems with built-in security costs

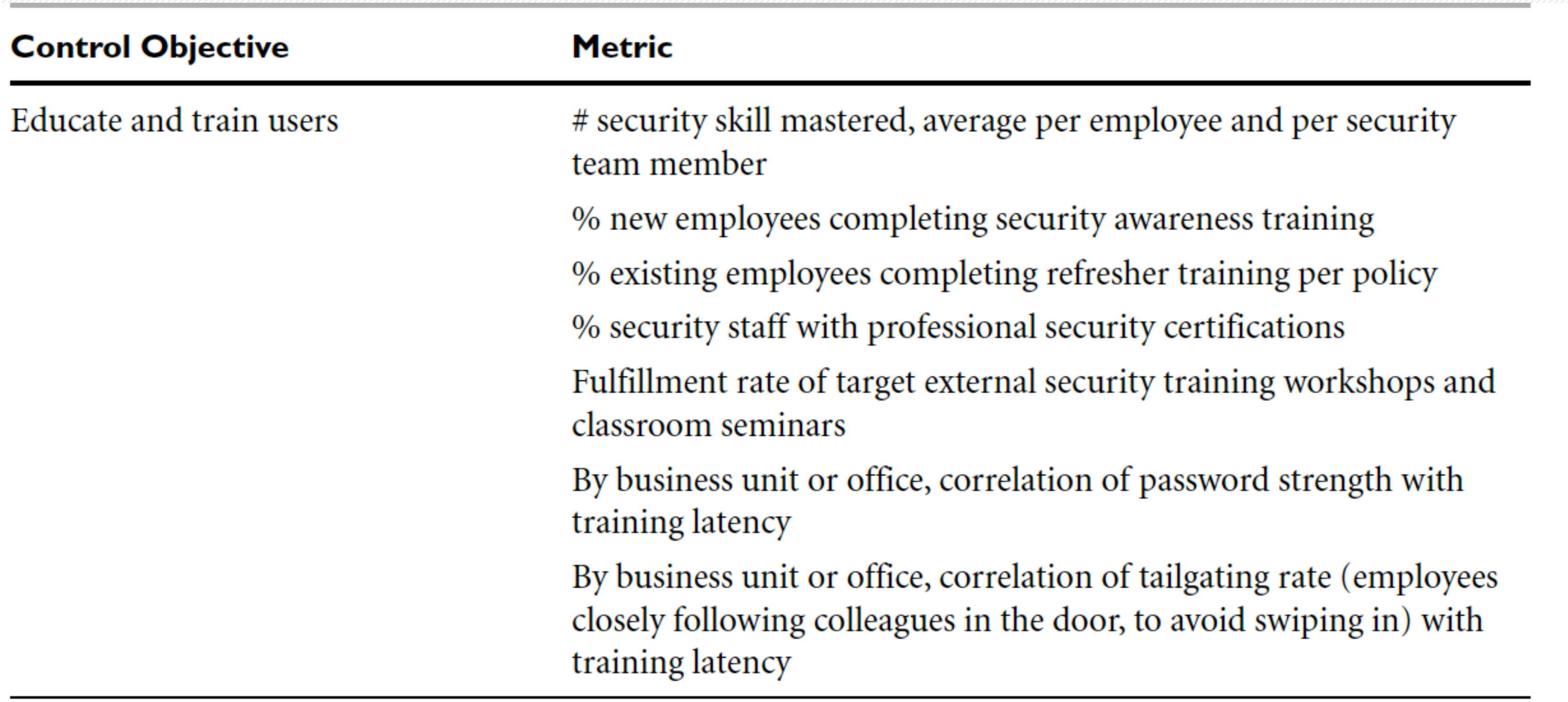
Acquisition and Implementation (3)

- Developing and maintaining procedures
  - Procedures for starting and stopping the system
  - Day-to-day operational responsibilities and tasks
  - Availability policy and expected service level
  - Monitoring and oversight responsibilities
  - Problem management processes
  - Business continuity and disaster recovery instructions
  - Technical architecture
  - Security responsibilities for users and operators
  - Data security policy
  - System ownership

Delivery and Support (1) –

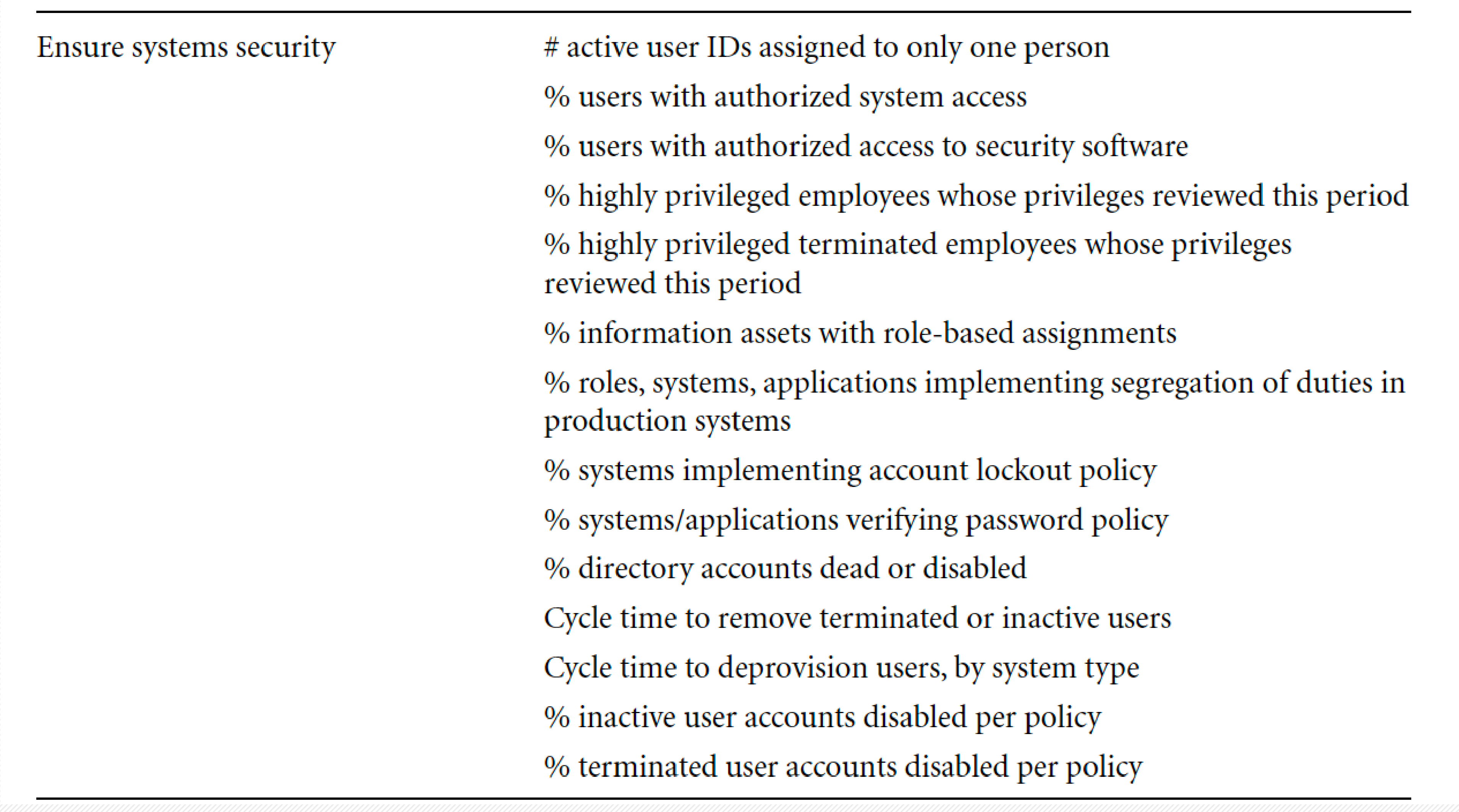
- The day-to-day control activities that comprise security operations

Delivery and Support (2) – Educate and train users



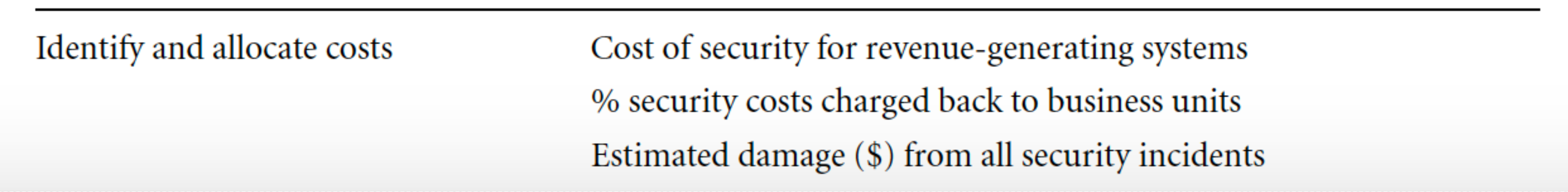
Control Objective	Metric
Educate and train users	# security skill mastered, average per employee and per security team member
	% new employees completing security awareness training
	% existing employees completing refresher training per policy
	% security staff with professional security certifications
	Fulfillment rate of target external security training workshops and classroom seminars
	By business unit or office, correlation of password strength with training latency
	By business unit or office, correlation of tailgating rate (employees closely following colleagues in the door, to avoid swiping in) with training latency

Delivery and Support (3) – Ensuring System Security



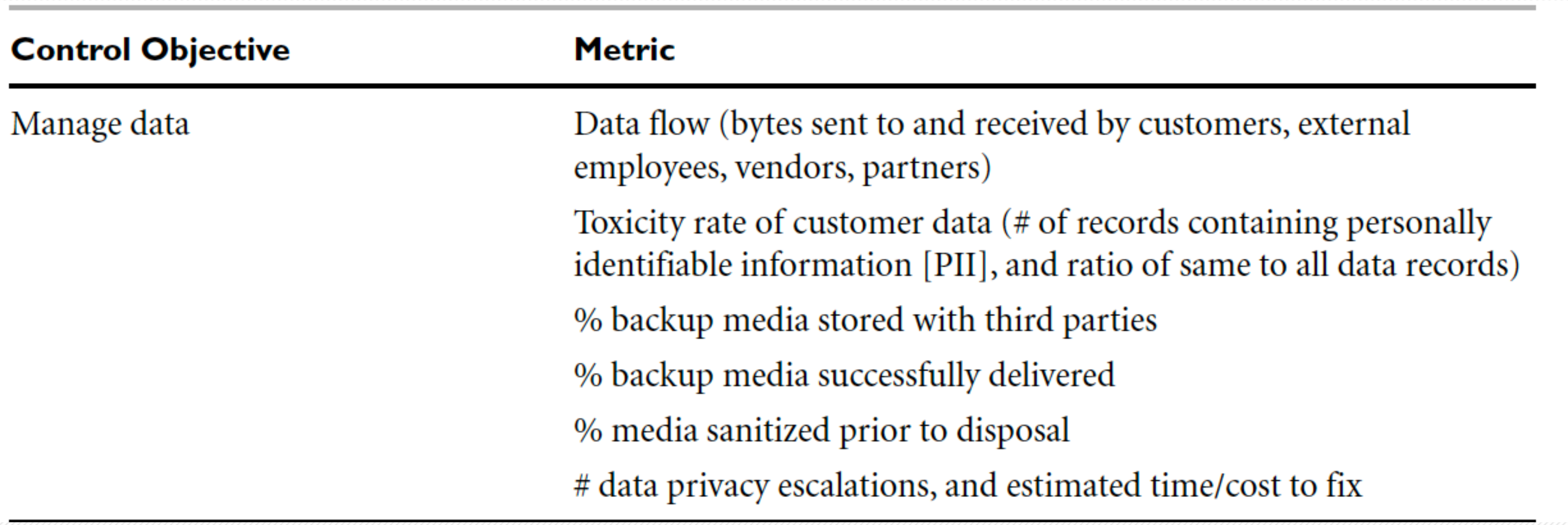
Ensure systems security	# active user IDs assigned to only one person
	% users with authorized system access
	% users with authorized access to security software
	% highly privileged employees whose privileges reviewed this period
	% highly privileged terminated employees whose privileges reviewed this period
	% information assets with role-based assignments
	% roles, systems, applications implementing segregation of duties in production systems
	% systems implementing account lockout policy
	% systems/applications verifying password policy
	% directory accounts dead or disabled
	Cycle time to remove terminated or inactive users
	Cycle time to deprovision users, by system type
	% inactive user accounts disabled per policy
	% terminated user accounts disabled per policy

Delivery and Support (4) – Identifying and Allocating Costs



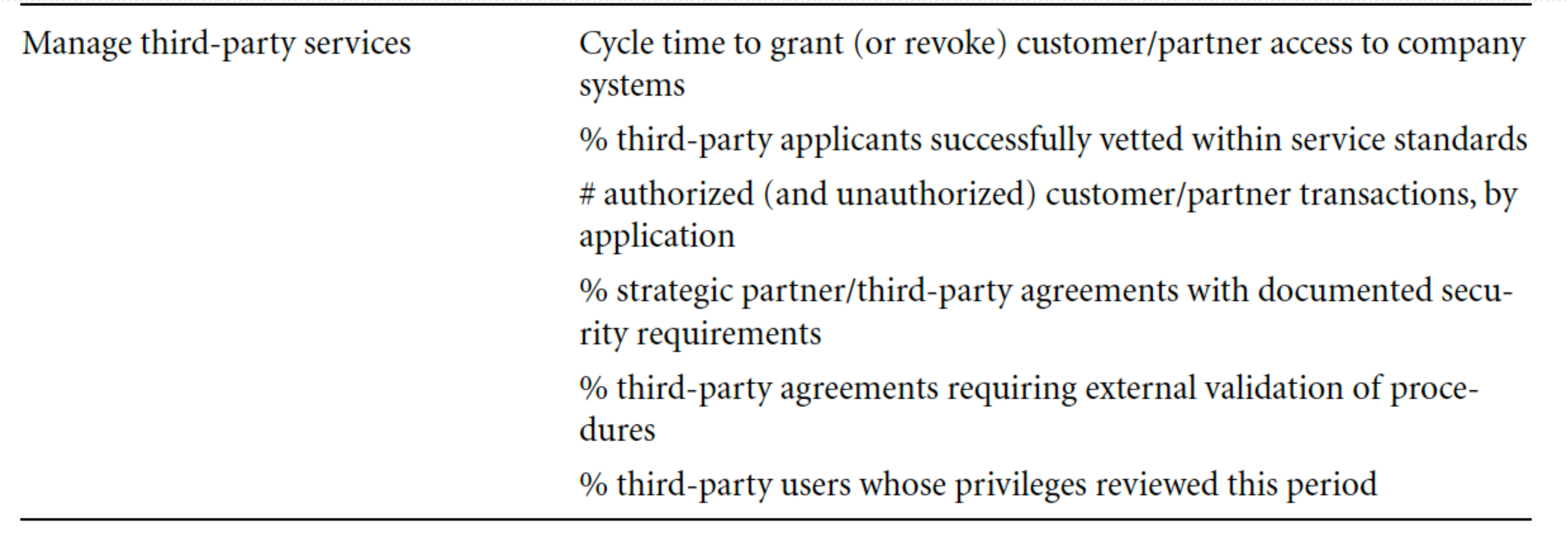
Identify and allocate costs	Cost of security for revenue-generating systems
	% security costs charged back to business units
	Estimated damage ($) from all security incidents

Delivery and Support (5) – Managing Data



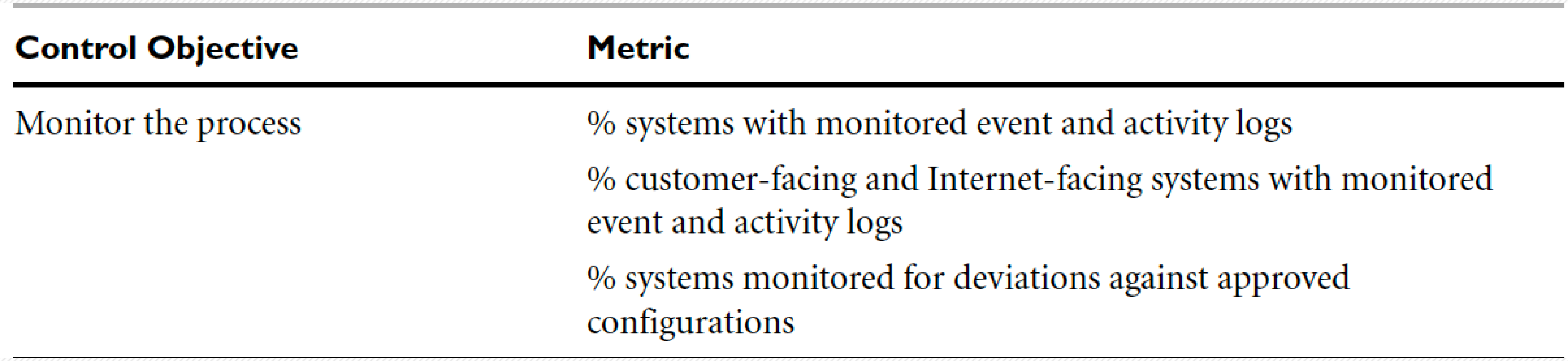
Control Objective	Metric
Manage data	Data flow (bytes sent to and received by customers, external employees, vendors, partners) Toxicity rate of customer data (# of records containing personally identifiable information [PII], and ratio of same to all data records) % backup media stored with third parties % backup media successfully delivered % media sanitized prior to disposal # data privacy escalations, and estimated time/cost to fix

Delivery and Support (6) – Managing 3rd Party Services



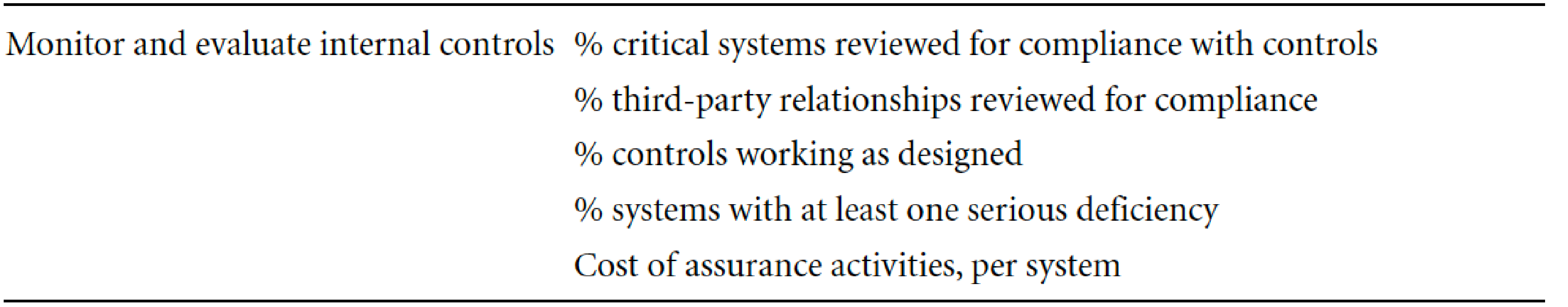
Manage third-party services	Cycle time to grant (or revoke) customer/partner access to company systems % third-party applicants successfully vetted within service standards # authorized (and unauthorized) customer/partner transactions, by application % strategic partner/third-party agreements with documented security requirements % third-party agreements requiring external validation of procedures % third-party users whose privileges reviewed this period

Monitoring (1)- Monitor the process



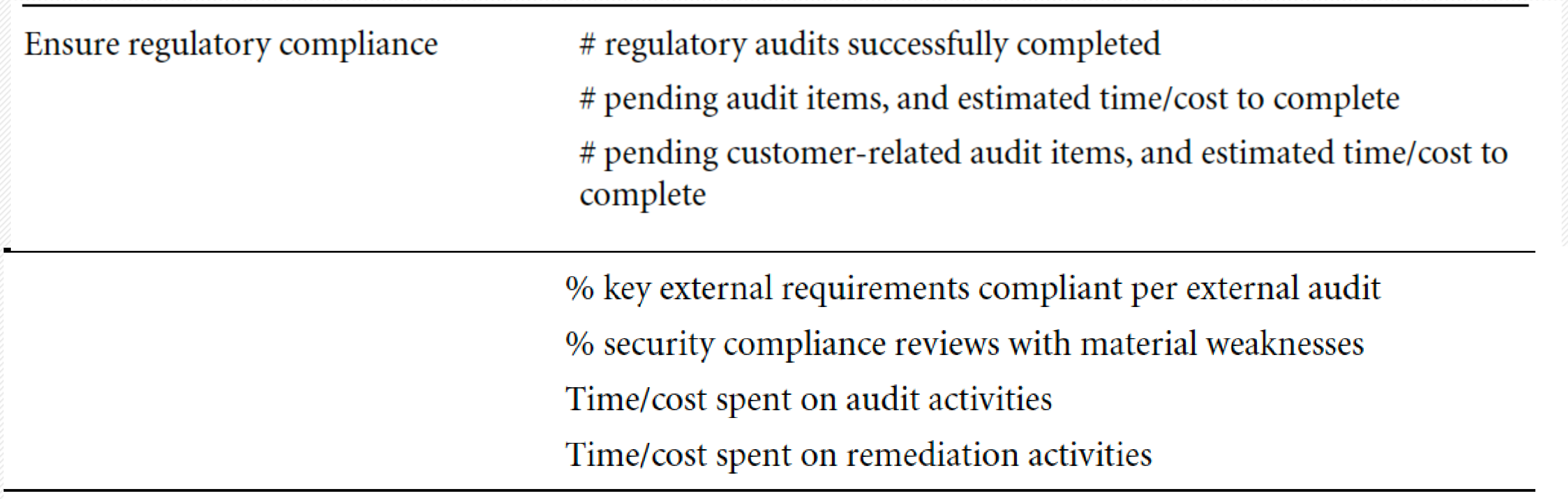
Control Objective	Metric
Monitor the process	% systems with monitored event and activity logs % customer-facing and Internet-facing systems with monitored event and activity logs % systems monitored for deviations against approved configurations

Monitoring (2)- Monitoring and Evaluating Internal Controls



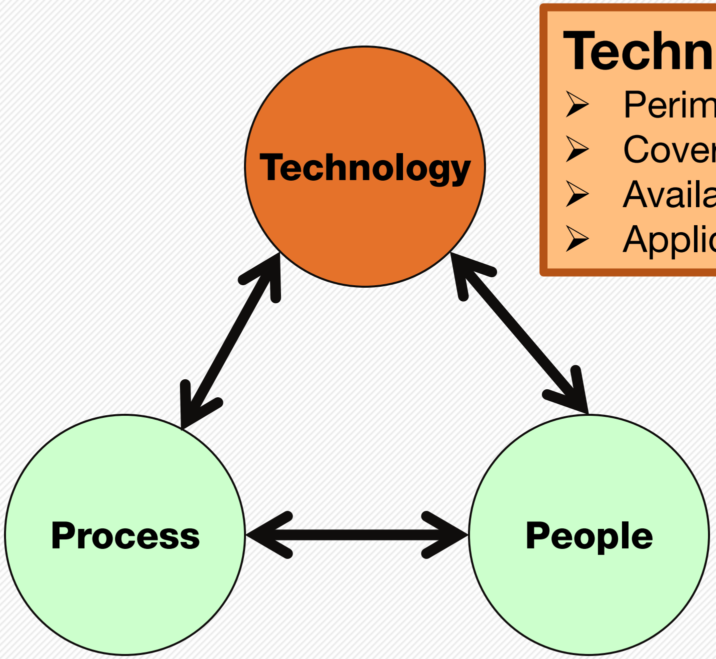
Monitor and evaluate internal controls	% critical systems reviewed for compliance with controls
	% third-party relationships reviewed for compliance
	% controls working as designed
	% systems with at least one serious deficiency
	Cost of assurance activities, per system

Monitoring (2)- Ensuring Regulatory Compliance



Ensure regulatory compliance	# regulatory audits successfully completed
	# pending audit items, and estimated time/cost to complete
	# pending customer-related audit items, and estimated time/cost to complete
	% key external requirements compliant per external audit
	% security compliance reviews with material weaknesses
	Time/cost spent on audit activities
	Time/cost spent on remediation activities

Security Metrics – Summary



Technology

Process

People

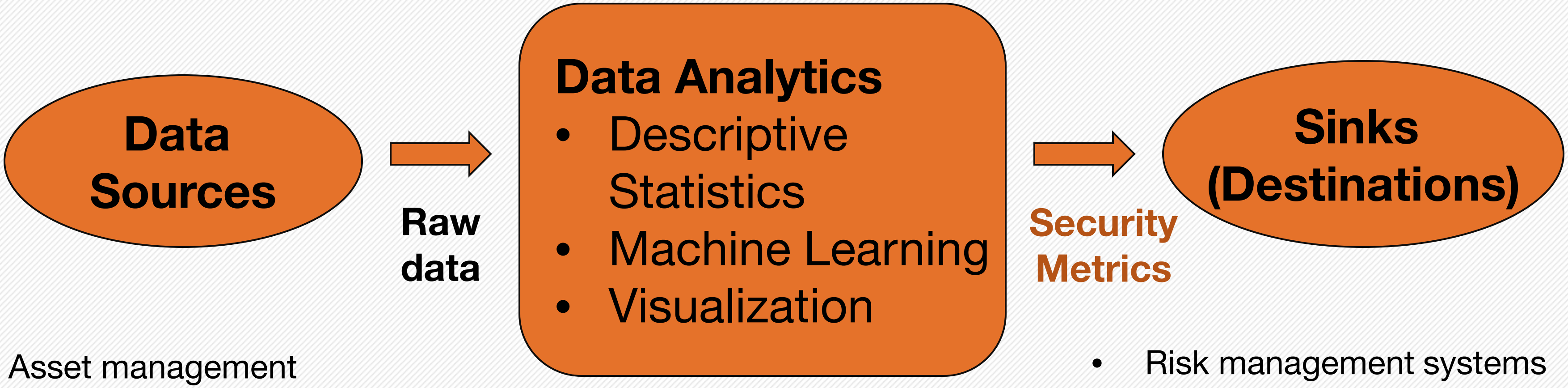
Technical Diagnostic Metrics

- Perimeter security & threats
- Coverage & control
- Availability & reliability
- Application security

Program Effectiveness Metrics

- Planning & organization
- Acquisition & implementation
- Delivery & support
- Monitoring

Data Sources and Sinks



Data Sources

Raw data

Data Analytics

- Descriptive Statistics
- Machine Learning
- Visualization

Security Metrics

Sinks (Destinations)

- Asset management
- Configuration management
- Patch management
- Network and system management
- Security vulnerability and event management
- Human resources (HR)
- Identity and access management (IAM)
- Customer relationship management (CRM)
- The Incident Response Center
- Policy Information
- Regulatory information
- Audit results

- Risk management systems
- Budget management
- Audit and compliance assessment systems
- Security operations
- General purpose reporting systems
- Scorecard management systems

Effective Security Metrics

- Often referred to as SMART, i.e. Specific, Measurable, Attainable, Repeatable and Time-dependent
- In the pursuit of metrics that meet SMART criteria, it is important to consider:
  - how difficult collection of accurate data might be for a given metric;
  - the potential that the metric might be misinterpreted;
  - the need to periodically review metrics that are being tracked and make changes as needed.

Accurate data collection

- Risk = Threat + Vulnerability + Value
  - Asset Value – easiest to measure in some cases, but difficult to quantify certain assets like institutional reputation
  - Threat – very hard to measure the potential for harm, although information from external sources may be useful
  - Vulnerability – automated computing device vulnerability tools provide good information, but not all vulnerabilities can be quantified

Potential Mis-interpretation

- Example: number of security breaches experienced by a specific entity or industry sector.
  - Not necessarily an indication of how secure an organization actually is
    - Certain security improvements may reveal security lapses that previously went undetected
    - This is a good thing.

Maturity of the overall security program

- The effectiveness of a given metric can vary depending upon:
  - The maturity of the overall security program
  - The maturity of a specific program component