The Role of IT Security

Jennifer L. Bayuk
jbayuk@bear.com

Securities Industry Association Internal Audit Division
October, 2003

BEAR STEARNS

IT Security

- **Literature Survey**
- **Process Definition**
- **Auditing the Function**

The Role of IT Security

Literature Survey

BEAR STEARNS

Academic Advice

"Strive for all major Infosec functions to be part of your Corporate Information Assets Protection Program (CIAPP)"

Have an Information Systems Security Strategic Plan (ISSSP), a document upon which to build CIAPP.

Information Security Officer responsibilities:

- **Manage people**
- **Manage CIAPP**
- **Manage CIAPP processes.**

COBIT Management Guidelines

IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimized and included in a verified *security plan*. Security functions are *integrated* with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using *automated active monitoring* approaches for critical systems. Incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic *security assessments* evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of *security incidents* and pro-active identification of risk is the basis for continuous improvements. *Security processes and technologies are integrated organization wide*.

CSO Magazine CISO Survey

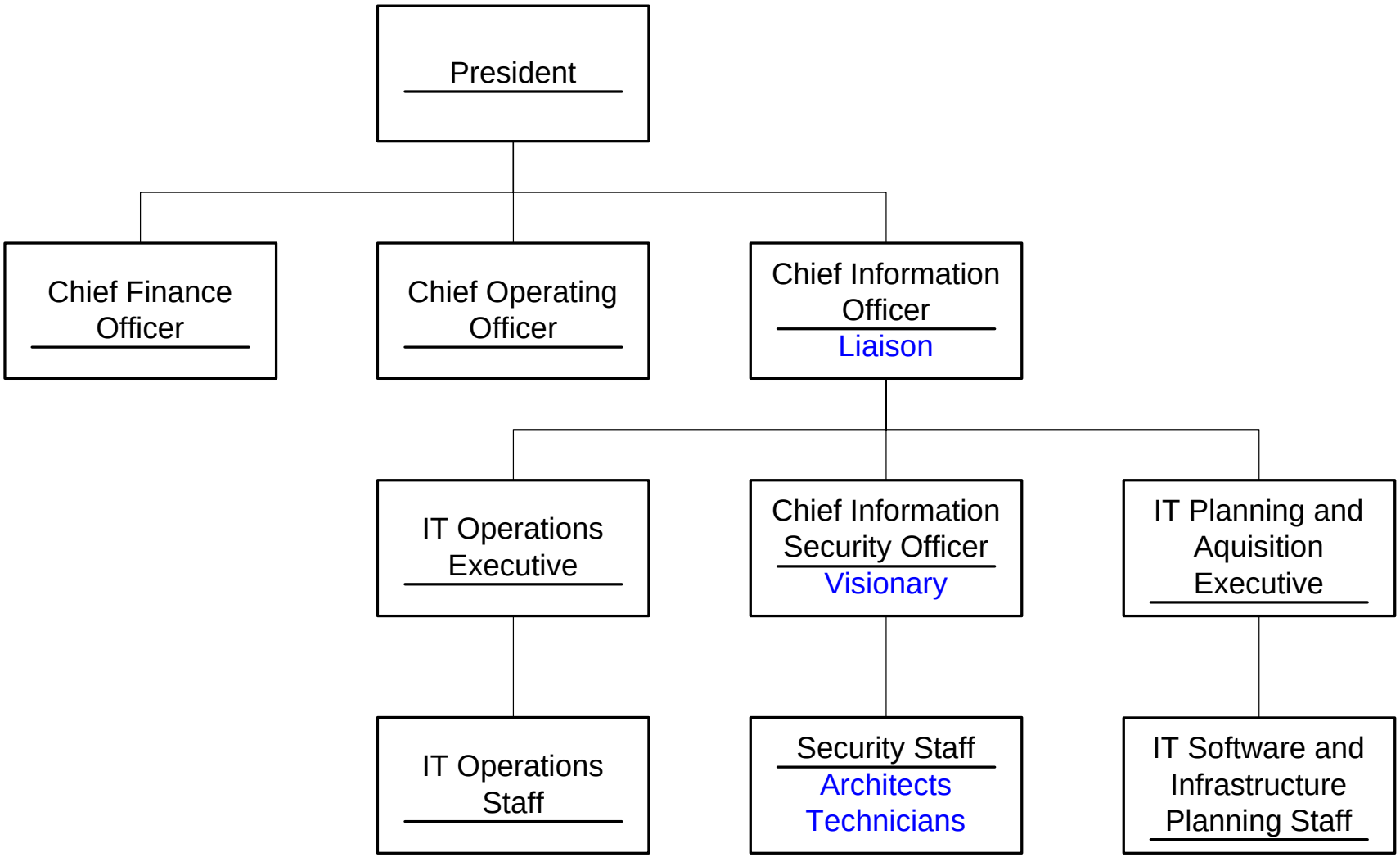
50% have non-security responsibilities, "almost as many names for top security executives as there are survey respondents," 86% first in job to hold title, 85% in job less than 5 years, 45% in job less than 2 years

So in 85% of organizations with CISOs, security responsibility has until very recently been distributed

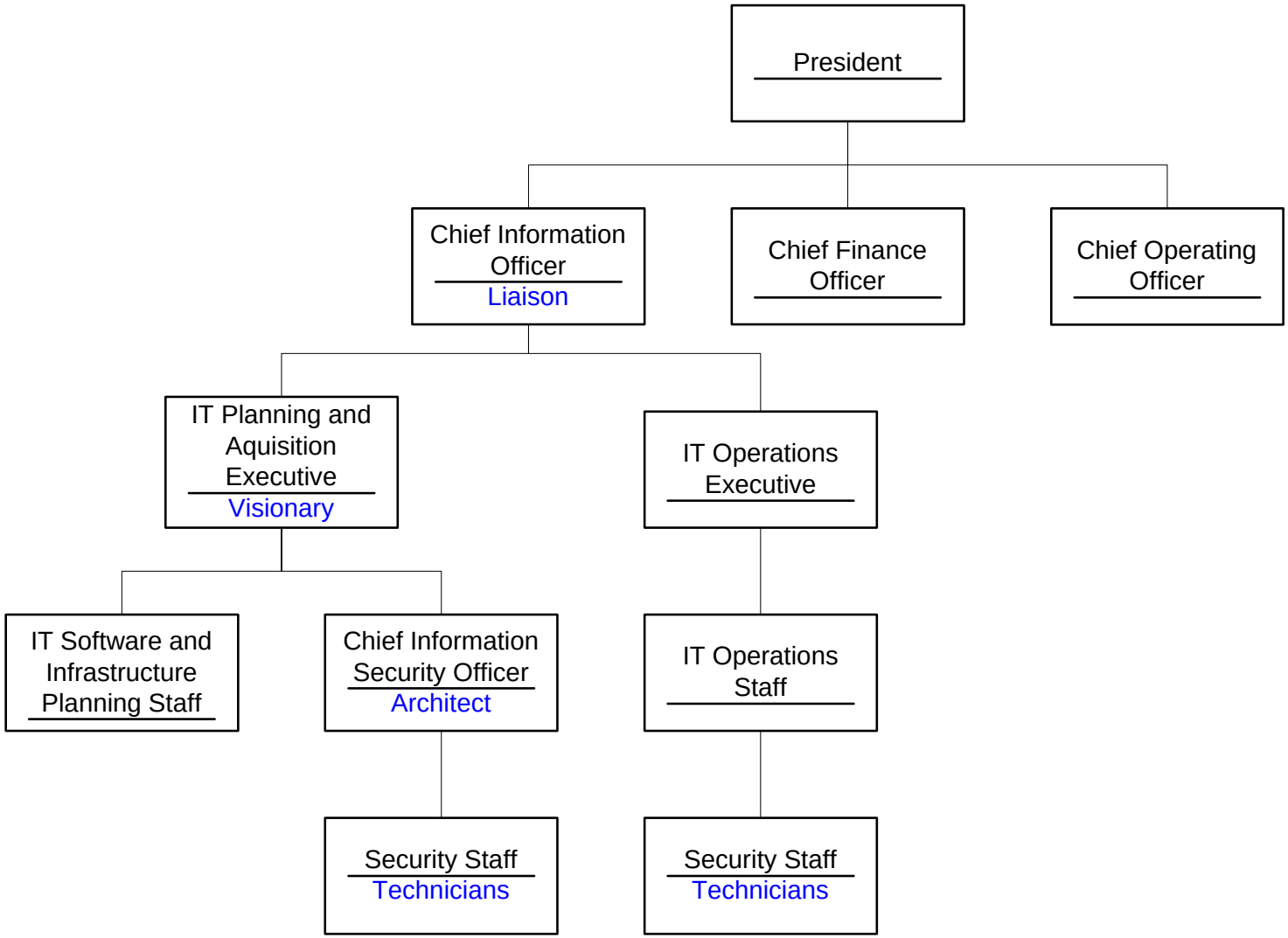
Example Responsibilities

Role:	Charter:	Could report to:	Day to day functions:
Liaison	Protect the digital integrity of the corporation	Chief Security or Information Officer	Maps business and regulatory requirements to a security model encompassing data, applications, and infrastructure
Visionary	Secure the information systems assets of the corporation	Chief Information Officer or Chief Architect	Produces policy, performs audit follow up, initiates projects, monitors statistics, and plans incident response.
Architect	Design and assist in the implementation of security solutions	Chief Architect or IT Planning Executive	Selects and integrates infrastructure and application product, produces technical requirements and design documents, implementation plans.
Technician	Establish and maintain security procedures, tools, and techniques	IT Operations Executive	Supervises direct and indirect reports in process and workflow that secures information systems resources.

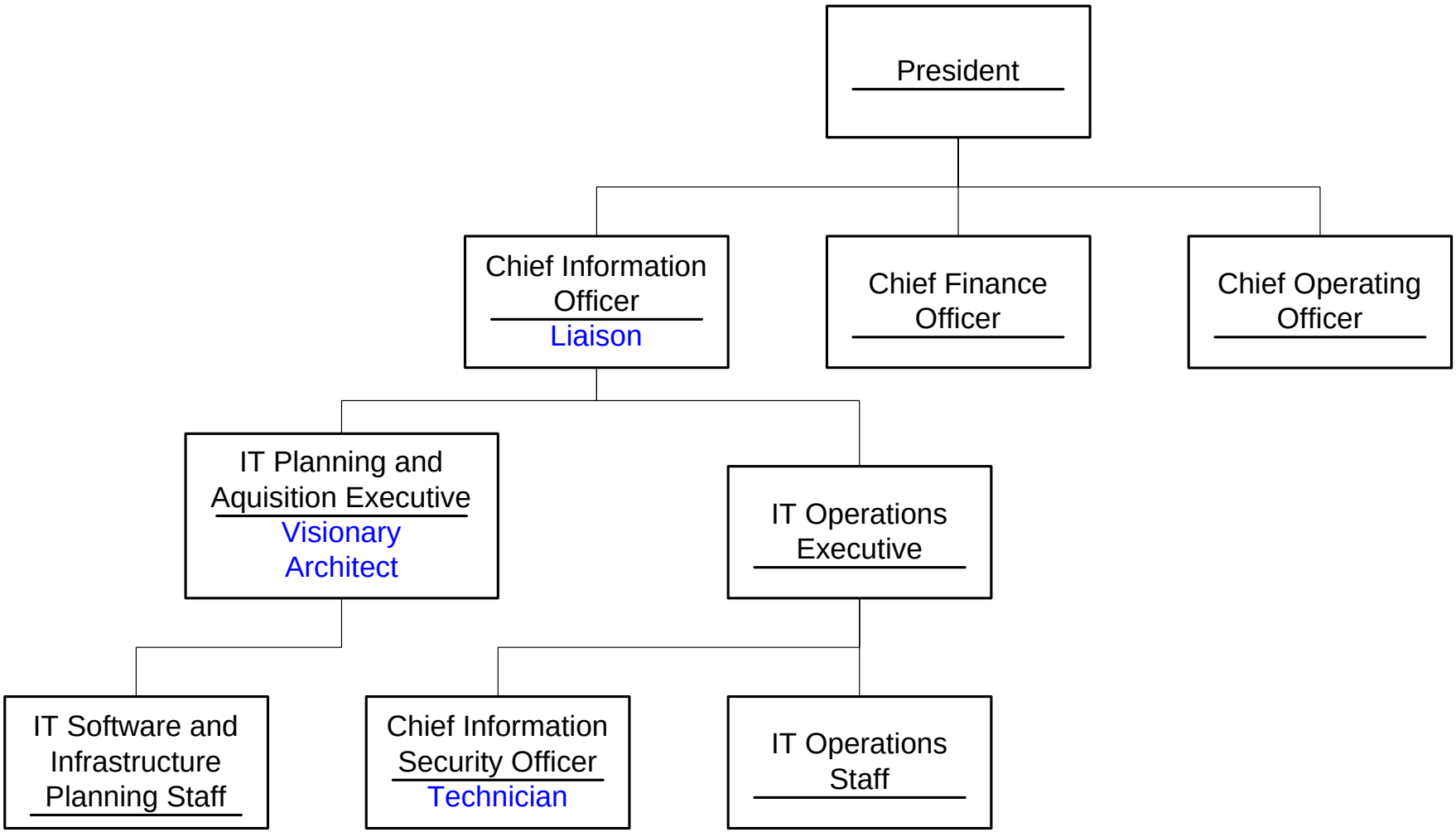
CISO as Visionary



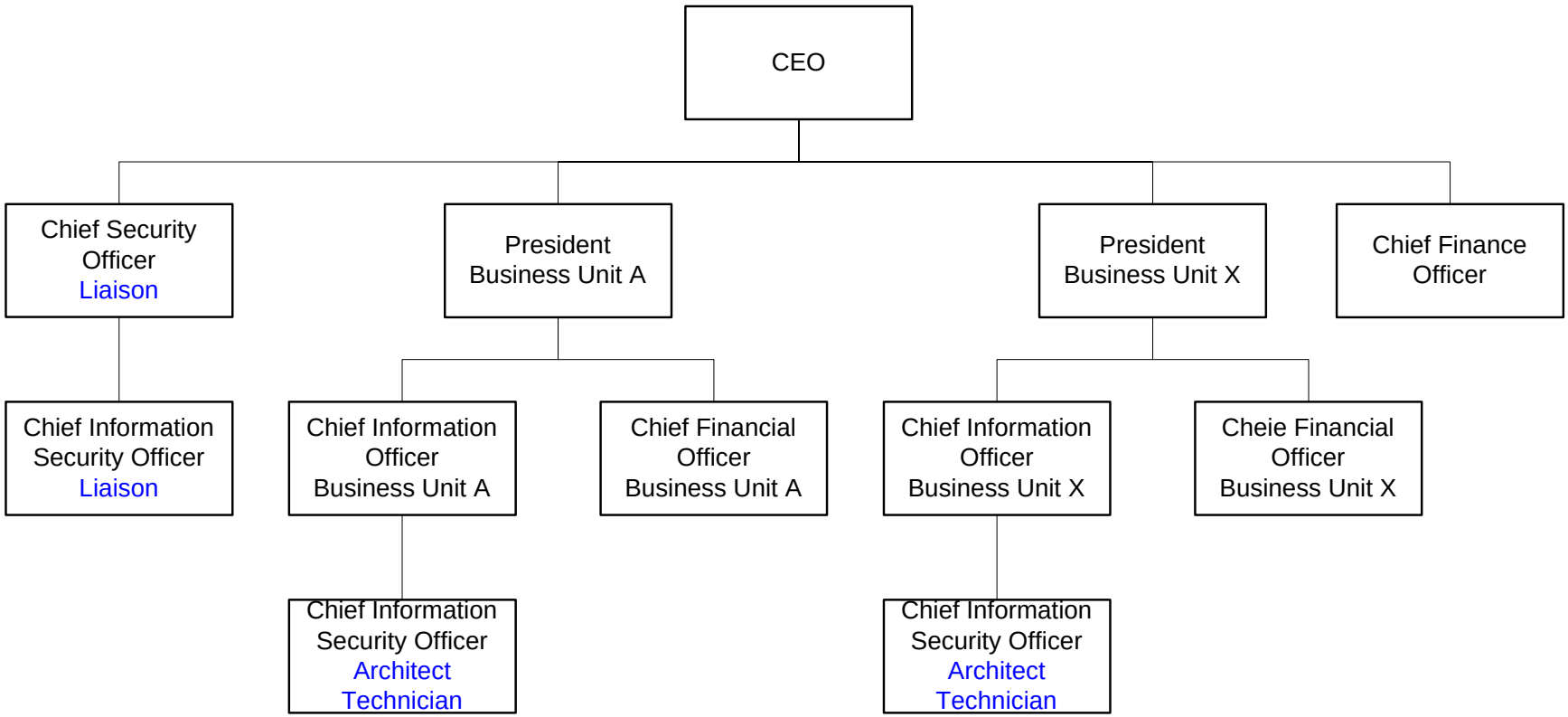
CISO as Architect



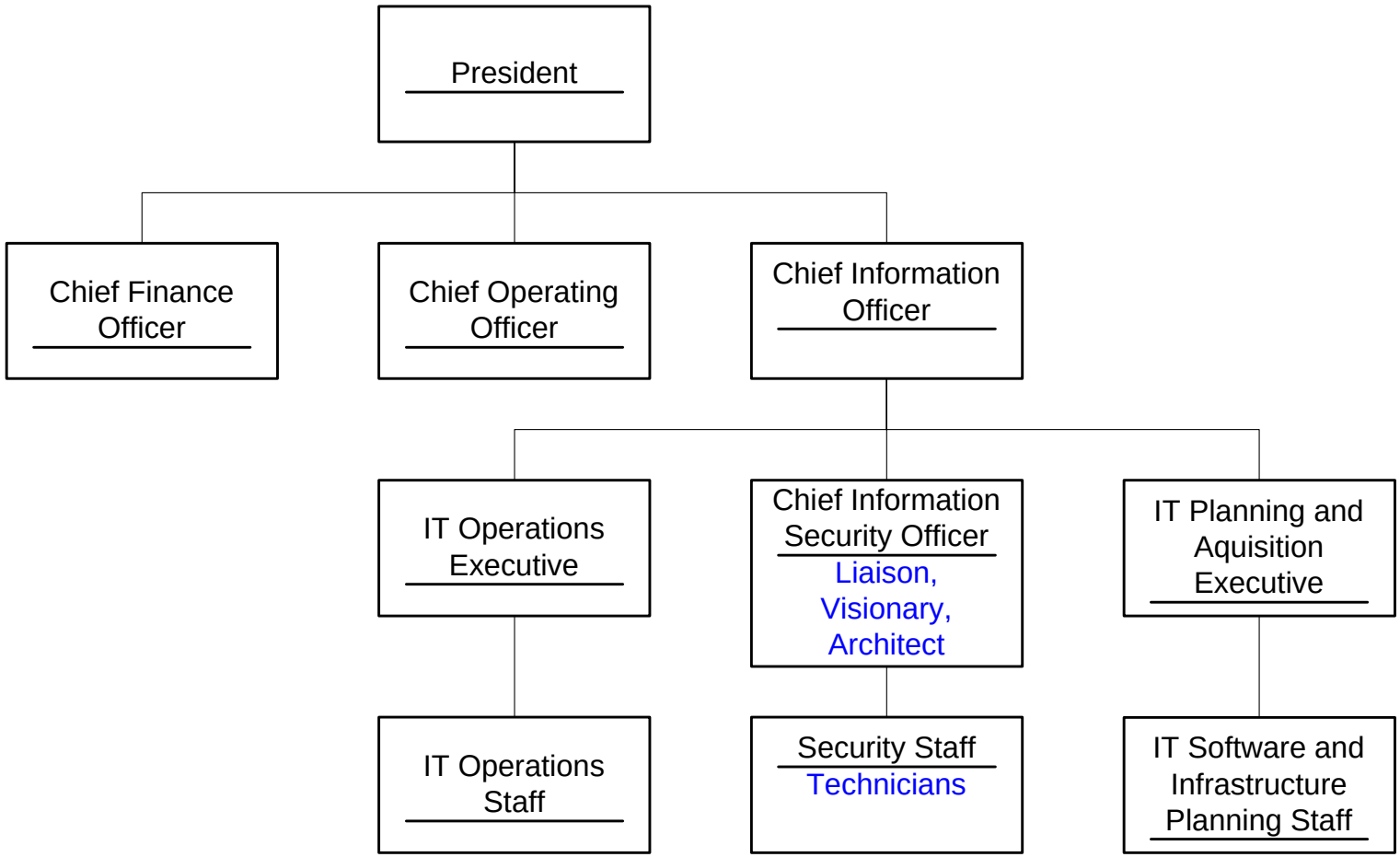
CISO as Technician



CISO as Cross-BU Liaison



CISO as Security Central



The Role of IT Security

Process Definition

BEAR STEARNS

Best Practice: Process Integration

- **Minimizes need for dedicated security staff**
- **Leverages platform administrator expertise for security goals**
- **Allows IT Security to concentrate on process and supporting architecture**
- **Does not require IT Security to have any specific organizational affiliation**

Additional Practical Rationale

- **All CISOs, even architects and technicians, end up responsible for Security Policy, yet a CISO that is an architect or a technician will not have the organizational clout to manage a CIAPP.**
- **Given the job functions that require unlimited access (e.g. data transfer, performance tuning, batch job scheduling), all Infosec-related functions will not be managed through CIAPP people and processes.**

Commonalities in IT Processes

Key Goal Indicators

Key Performance Indicators

Level of Maturity

Level of Commitment

Examples of IT Processes (COBIT)

PLANNING AND ORGANISATION
PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Organisation and Relationships
PO5 **Manage the IT Investment**
PO6 Communicate Management Aims and Direction
PO7 Manage Human Resources
PO8 Ensure Compliance with External Requirements
PO9 Assess Risks
PO10 Manage Projects
PO11 Manage Quality

P05

ACQUISITION AND IMPLEMENTATION
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Develop and Maintain Procedures
AI5 Install and Accredit Systems
AI6 Manage Changes

DELIVERY AND SUPPORT
DS1 Define and Manage Service Levels
DS2 Manage Third-Party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Assist and Advise Customers
DS9 Manage the Configuration
DS10 Manage Problems and Incidents
DS11 Manage Data
DS12 Manage Facilities
DS13 Manage Operations

MONITORING
M1 Monitor the Processes
M2 Assess Internal Control Adequacy
M3 Obtain Independent Assurance
M4 Provide for Independent Audit

P05 Key Goal Indicators

- **Percent of IT investments meeting or exceeding expected benefits, based on return on investment and user satisfaction**
- **Actual IT expenses as percent of total organization expenses vs. target**
- **Actual IT expenses as a percent of revenues vs. target**
- **Percent of business owner IT budgets met**
- **Absence of project delays caused by lags in investment decisions or unavailability of funding**

P05 Key Performance Indicators

- **Percent of projects with business owners**
- **Months since last review of budgets**
- **Time lag between deviation occurrence and reporting**
- **Percent of project files containing investment evaluations**
- **Number of projects where business benefits are not verified post-facto**
- **Number of projects revealing investment or resource conflicts after approval**
- **Number of instances and time-lag in delayed use of new technology**

Security Maps to IT Process

- **Returns on investment may not be met if the costs of implementing security requirements are not considered**
- **Security concerns of users, third parties, or internal data owners may cause project delays**
- **New technology may introduce unexpected infrastructure vulnerabilities that create resource conflicts**

Example – New Desktop Request

- User requests desktop program from dedicated desktop admin
- Admin checks “approved” list, requested program is not there
- Admin advises user to make formal request through software acquisition process
- Software acquisition process requires desktop engineering approval
- Control point within desktop engineering approval is “security review”
- Security reviews request, bringing admin and/or back for configuration consultation if required

D05: Ensure Systems Security

"Manage Security Measures" is covered by process integration, its practice should result in:

1. **Identification, Authentication, and Access**
2. **Security of Online Access to Data**
3. **User Account Management**
4. **Management Review of User Accounts**
5. **User Control of User Accounts**
6. **Security Surveillance**
7. **Data Classification**
8. **Central Identification and Access Rights Management**
9. **Violation and Security Activity Reports**
10. **Incident Handling**
11. **Reaccreditation**
12. **Counter-Party Trust**
13. **Transaction Authorization**
14. **Nonrepudiation**
15. **Trusted Path**
16. **Protection of Security Functions**
17. **Cryptographic Key Management**
18. **Malicious Software Prevention, Detection and Correlation**
19. **Firewall Architectures and Connections with Public Networks**
20. **Protection of Electronic Value**

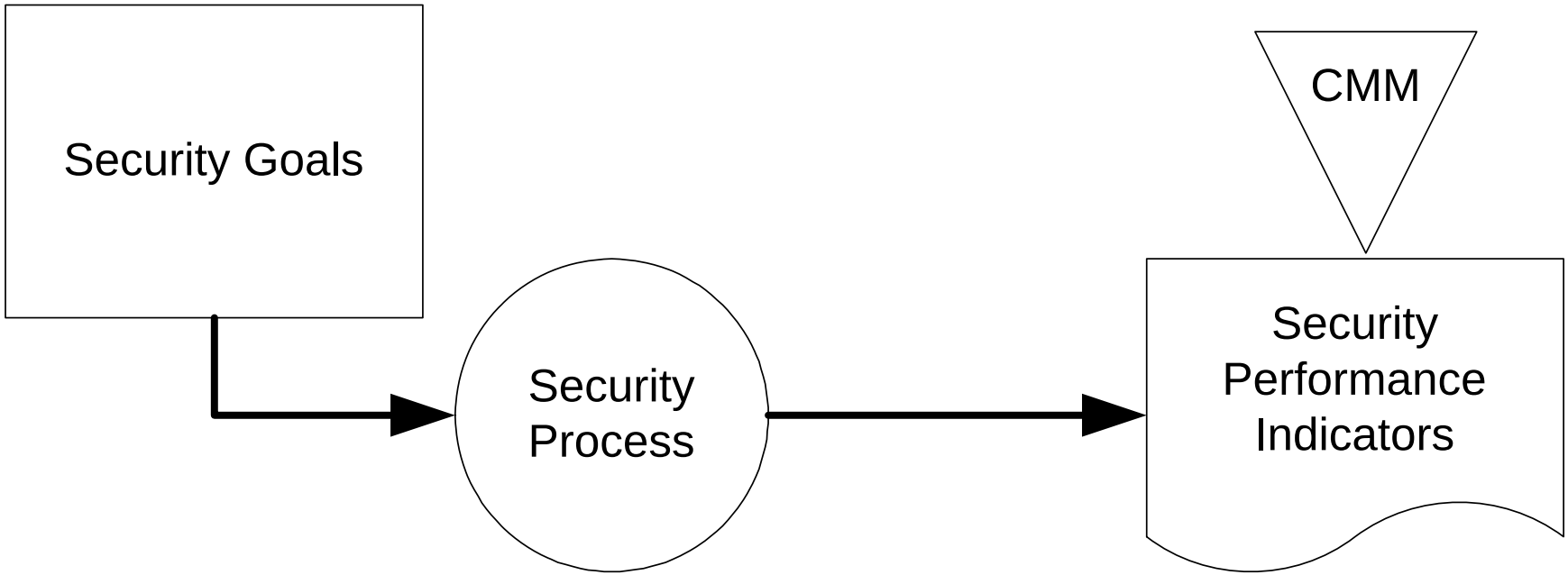
Best Practice: Automated Verification

- **Minimizes need for dedicated security operations**
- **Leverages existing incident response and escalation procedures**
- **Allows IT Security to concentrate on improving results**

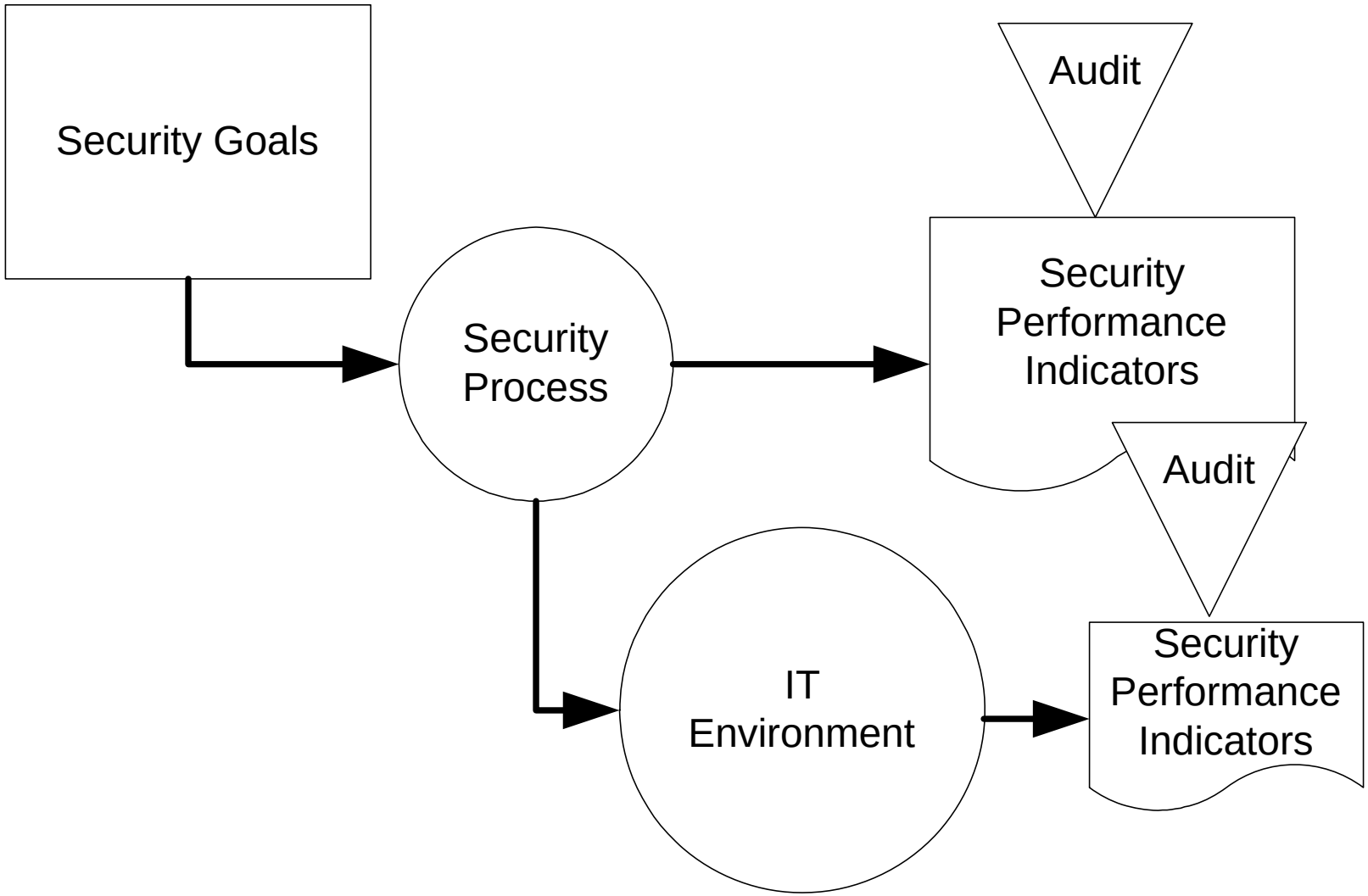
Security Measurement Types

Security Assessment Model Comparison					
Assessment Model Type:	Utilizes as evaluators:	Evaluators' standards consist of…	Measurement activity consists of…	There is a tacit assumption that…	Metrics produced are…
Capability Maturity	consultants and quality analysts	…process requirements	…identifying the process by which security is achieved, then determining the extent to which the process is mature (for example, is it quantifiable and/or does it continuously improve).	… organizations committed to securing their infrastructure will formally adopt a process for so doing.	…organizational ratings.
External Audit	Independent Third Parties	…best practices	…comparing the level of management's control over the current systems infrastructure to that which would result if best practices were followed.	… there are "best practices" available on how to secure a given infrastructure.	…vulnerability listings.
Internal Audit	Internal reports to the Board of Directors	… control objectives set by management	…determining the extent to which management-defined controls are appropriate and if in fact they are followed.	… management has adopted a set of control objectives designed to secure information systems assets.	…vulnerability listings.
Risk Analysis	accountants	…dollars spent in like organizations	…comparing the dollar value at risk from potential harm to a system to the cost of implementing security.	… there is a known dollar figure that represents how much it would cost to "completely secure" the IT infrastructure.	… spending recommendations.
Strict Compliance	technologists	…maximally restrictive configuration parameters	…quantifying measurable parameters inherent in an IT infrastructure that reflect its "security profile."	… there are specific measurable parameters inherent in an IT infrastructure that reflect its "security profile."	…summary of measured variables.

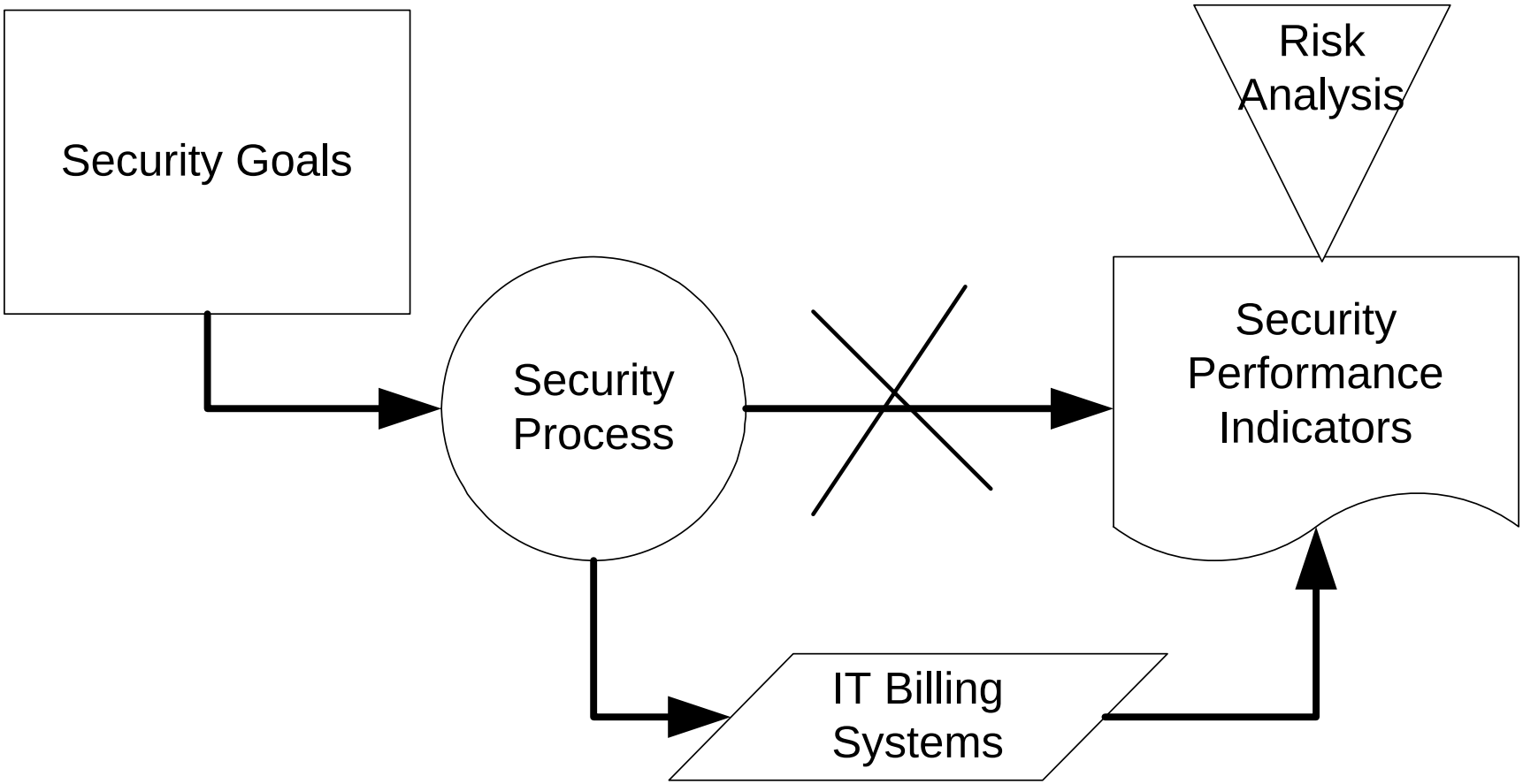
Capability Maturity



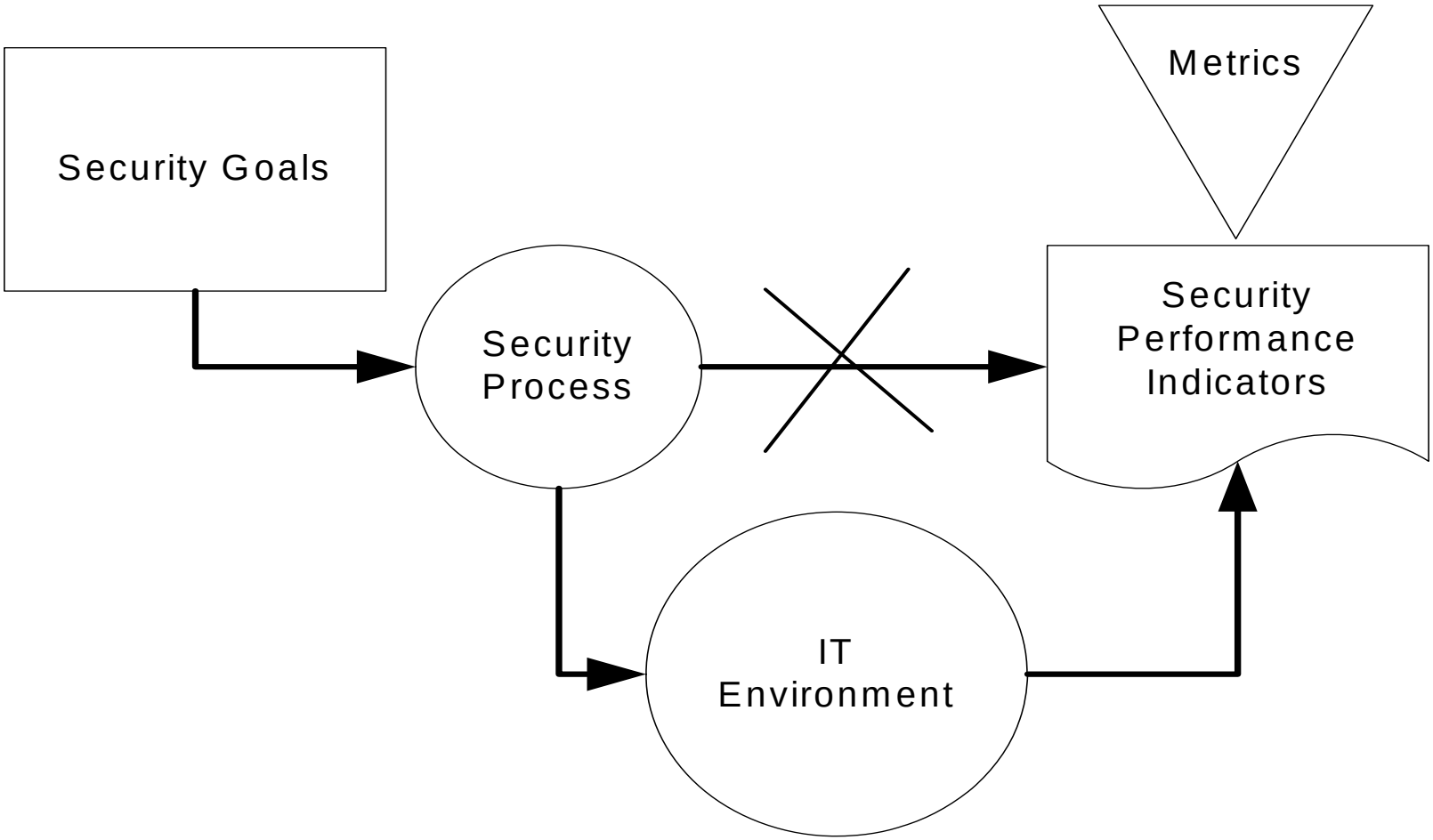
Audit


Security Goals
Audit
Security Process
Security Performance Indicators
Audit
IT Environment
Security Performance Indicators

Risk Analysis



Strict Compliance



Security Testing Example

Method: → Criterion: Identification, Authentication, and Access	Ask Management	Review Documentation	Spot checking	Penetration Test	Automated Verification
All users of the LAN are employees.	Questionnaire	Review procedures by which LAN IDs are added or removed.	Take a statistical sampling of LAN IDs. Look them up in the payroll system.	Try to guess LAN user names and passwords using user names that do not correspond to employees.	As part of the process to add a user, store the unique index from the payroll system in LAN user record, run a program to verify that these index match active payroll records.

Increase in assurance

The Role of IT Security

Auditing the Function

BEAR STEARNS

Auditing the IT Security Function

Prevention:	**Security processes and assignment of formal accountability for compliance**
Detection:	**Monitoring of compliance**
Recovery:	**Incident investigation**

Prevention Performance Indicators

- **Policy is clear for all platforms and standards are clear for platforms where risk levels are high or distributed administration is prevalent**
- **Security review and approval is part of the System Software and Architecture Lifecycle, especially with respect to security software selection and configuration, and new network connectivity**
- **Configuration change control is monitored**
- **User administration processes are controlled**

Detection Performance Indicators

- **Security metrics are clearly defined in advance of deployment**
- **Security metrics are automated as part of the system development lifecycle**
- **Security metrics are automatically collected and reviewed**

Recovery Performance Indicators

- **Security measurements are monitored and investigation occurs for security-related events**
- **Security events may be reported outside of that process**
- **There exists a documented and logged process for investigating and escalating security events**

The Role of IT Security

Jennifer L. Bayuk
jbayuk@bear.com

Securities Industry Association Internal Audit Division
October, 2003

BEAR STEARNS