ERCOT Information Security Strategy

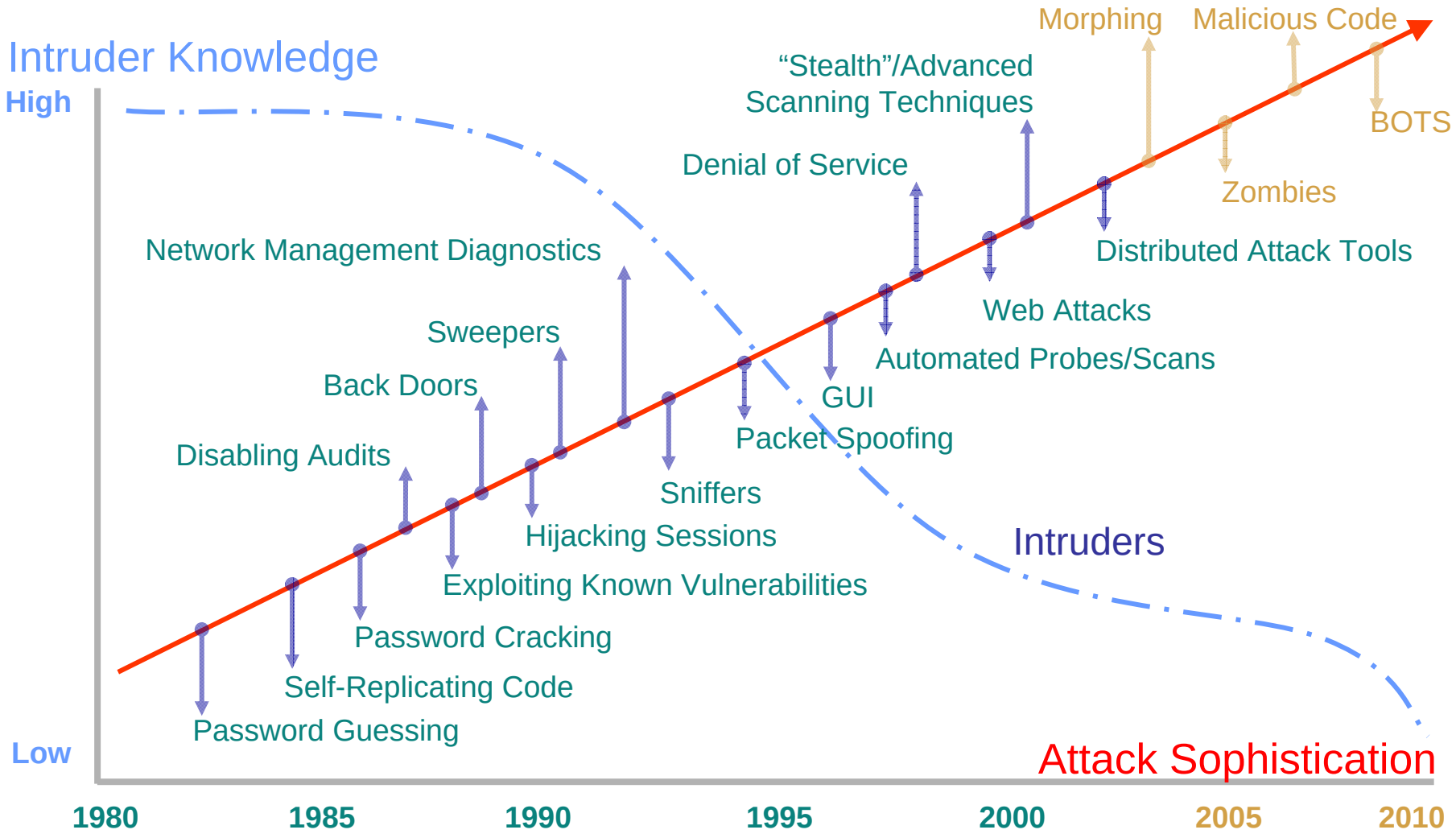
Ann Delenela, CISSP CISM

Information Systems Security Manager

Overview

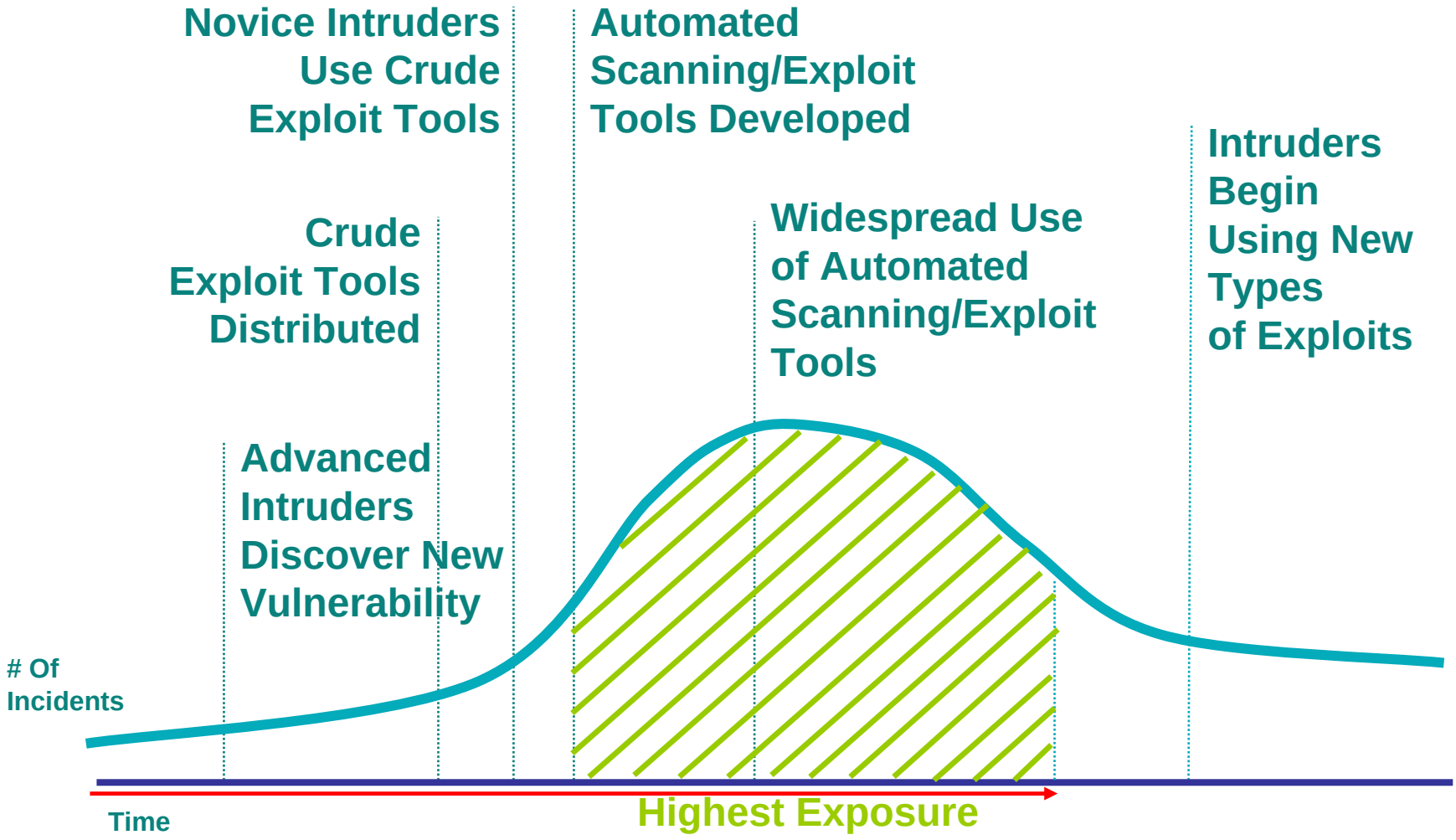
- Threats & Vulnerabilities
- Security Management Framework
- Protection Strategy
- ERCOT Information Security Mission Statement & Organization
- Information Security Roadmap
- Security Maturity Model

Attack Sophistication vs. Intruder Knowledge



Sources: Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005

Vulnerability Exploit Cycle



Source: Federal Bureau of Investigation

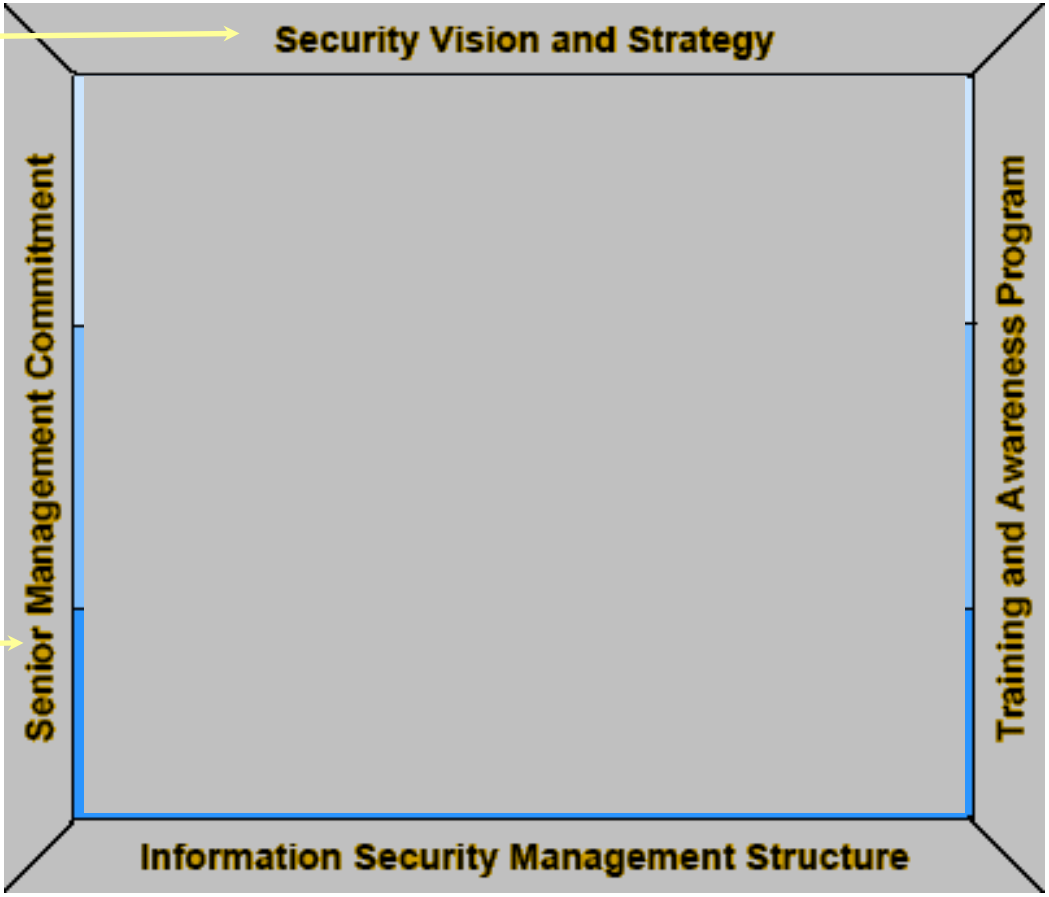
Information Security Management Framework

1) Security Vision & Strategy:

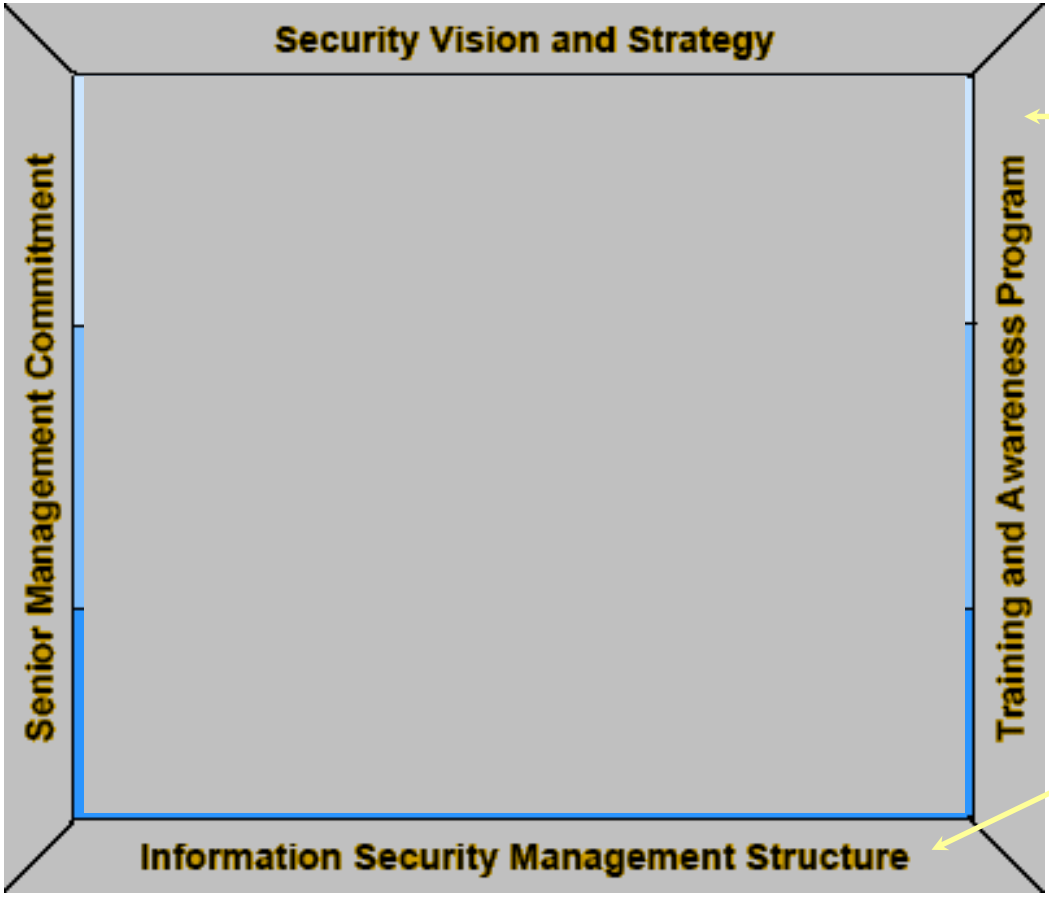
- Mission Statement, guiding principles
- Strategy for addressing information protection
- Security/Executive committee as an authoritative decision & communication vehicle

2) Sr. Mgmt Commitment:

- Commitment in principle & practice
- Support through policy, directives & resource allocation
- Determination of risk tolerance



Information Security Management Framework



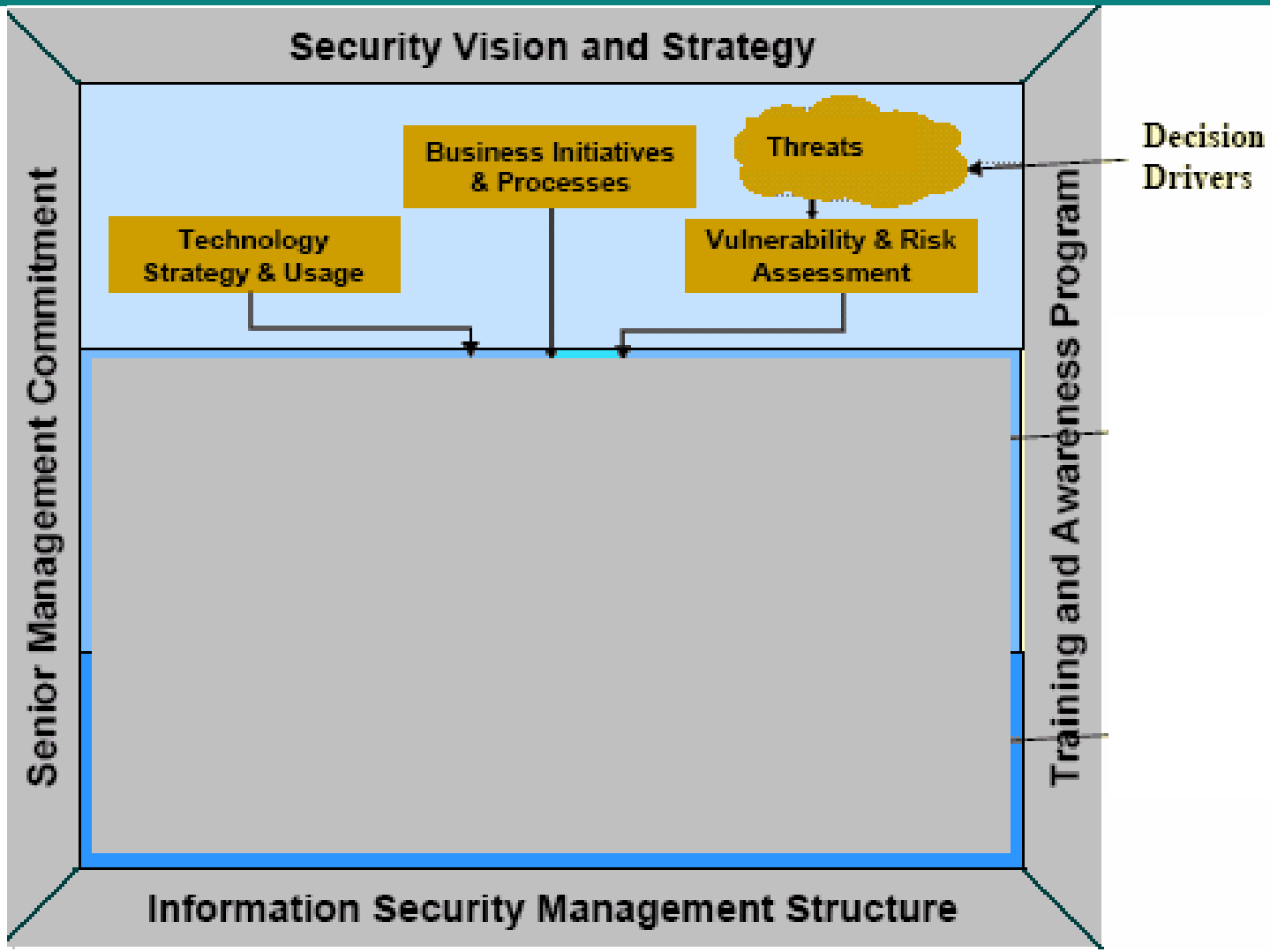
4) Training & Awareness Program:

- Communication covers all levels of organization and all aspects of information security
- Continuous, pervasive and an integral part training plans

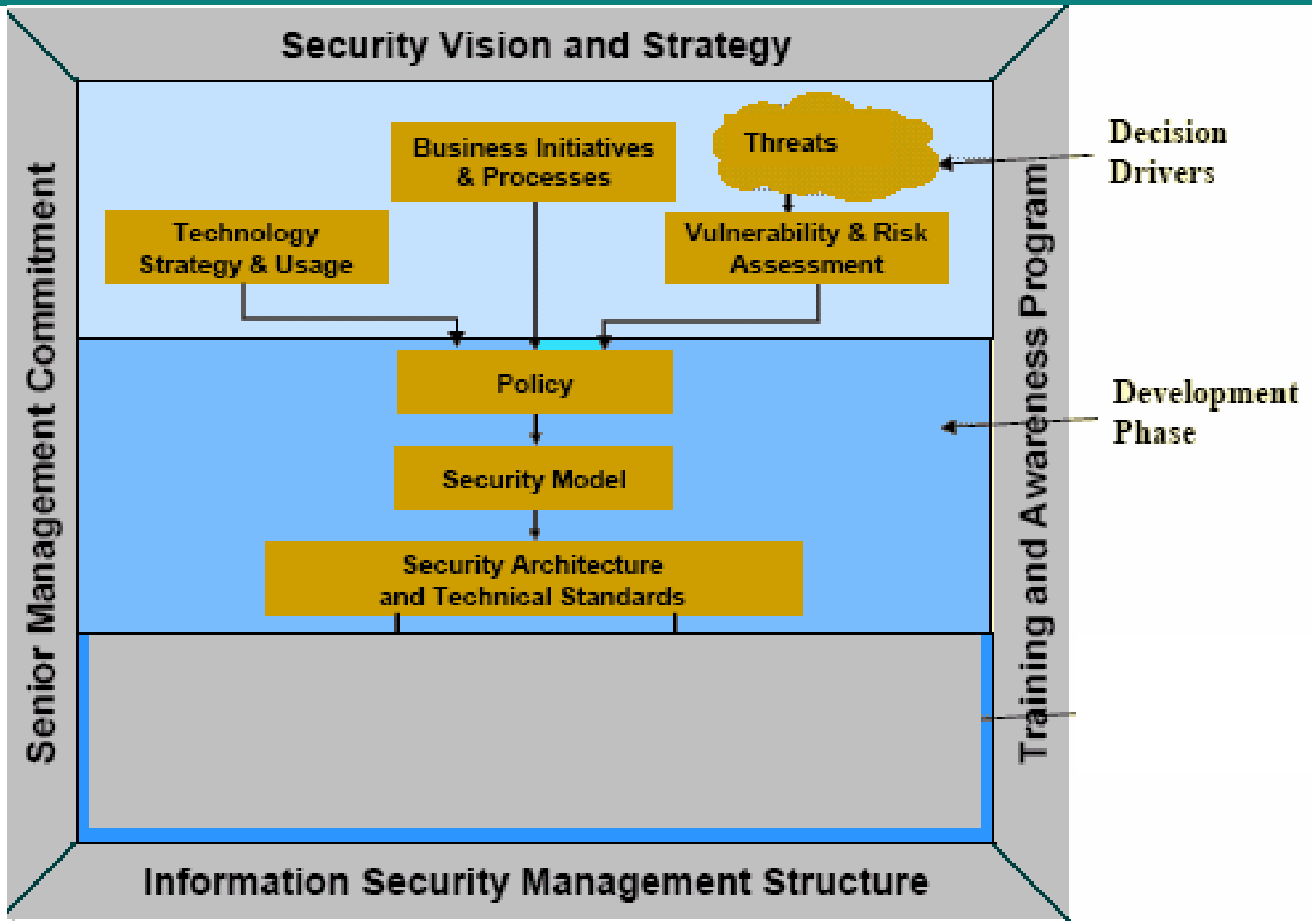
3) Security Mgmt Structure:

- Centralized & Decentralized resource deployment
- Cross functional roles and responsibilities

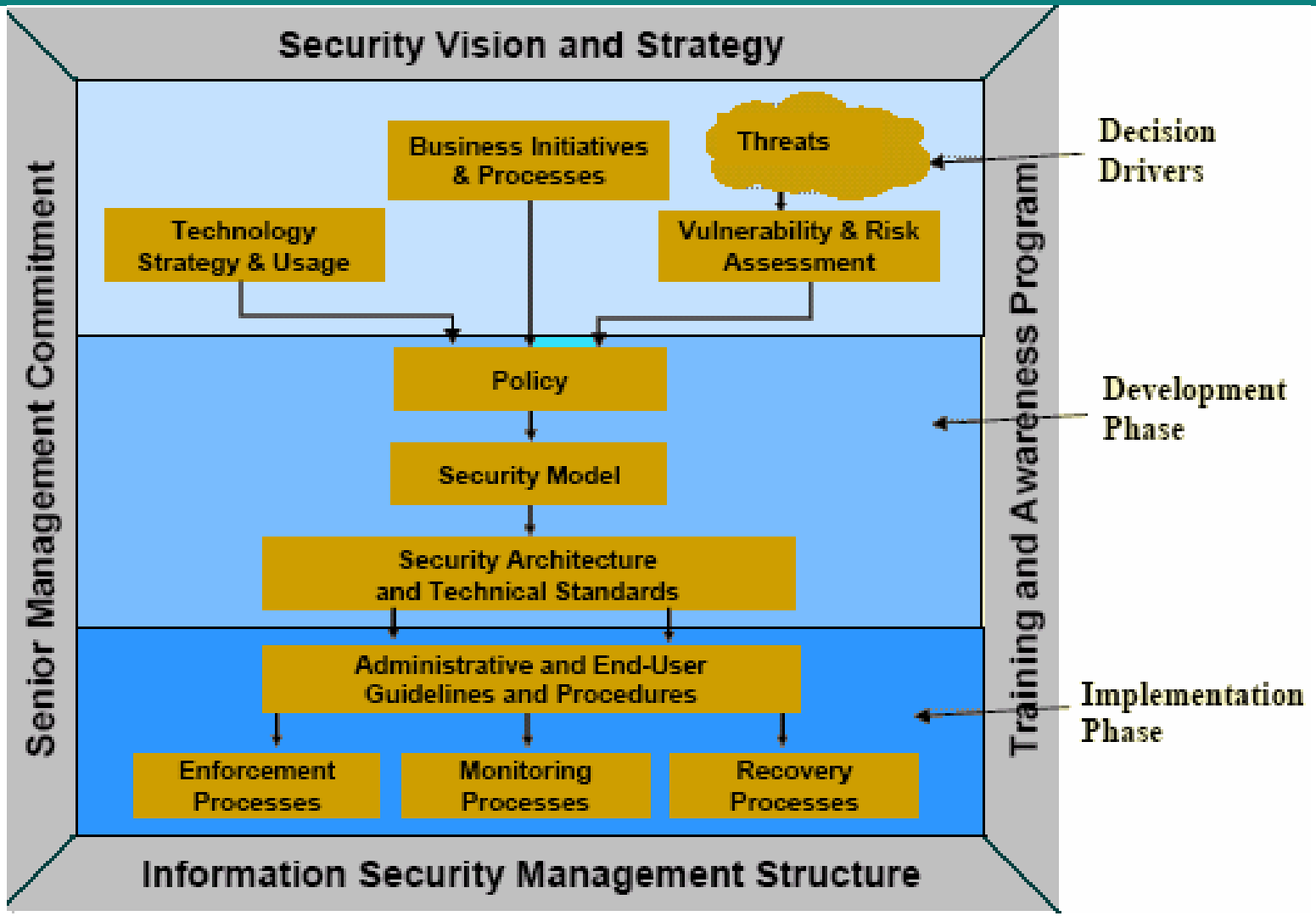
Information Security Management Framework



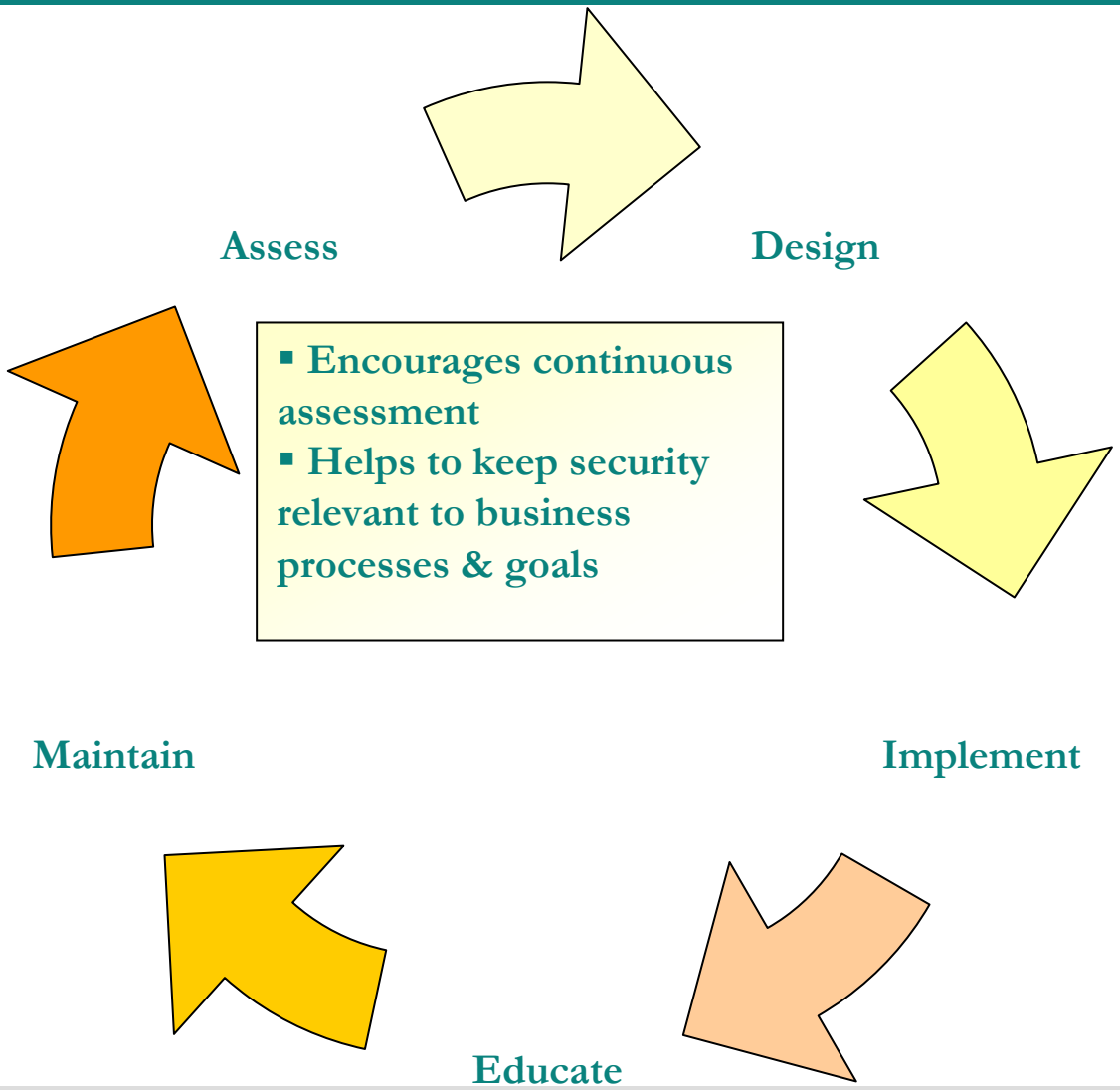
Information Security Management Framework



Information Security Management Framework



Security Lifecycle



Protection Strategy

Forensics

Monitoring
SIRT
Alerts

Response

Vuln Scanners
Monitoring Tech
Server Compliance
DB Compliance
IDS

Risk Mgmt
Patch Auditing
Access Review

Process
Compliance

Detection

Firewalls
Anti(V/S/A)
Patch Mgmt
IPS
Web Filtering
Email Security

Encryption
Host IPS
Proxies
Access Management

Policies
Standards
Processes
Awareness
Education

Prevention

GOVERNANCE:
- POLICY
- PROCESS
- COMPLIANCE

AWARENESS
EDUCATION

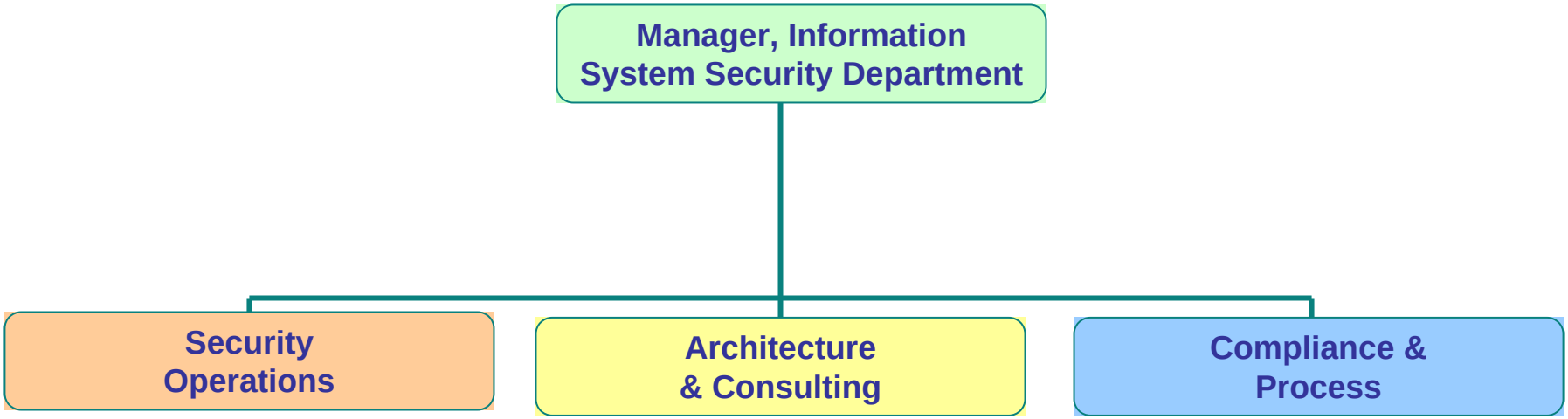
ISSD Mission Statement

The Information Systems Security Department's mission is to protect assets owned by and entrusted to ERCOT and enable ERCOT's business objectives.

To accomplish our mission, we commit to:

- Add value to the business through the development and delivery of cost beneficial asset protection programs
- Proactively focus on identification and mitigation of risk
- Seamlessly integrate security into business operations
- Respond in a timely and effective way to incidents that threaten the safety, security, integrity or availability of ERCOT's assets
- Conduct our security program in a manner that demonstrates the highest ethical standards
- Provide excellence in customer service
- Continually practice quality in our craft

ISSD Organization



Security Outreach - Advisory Groups & Committees

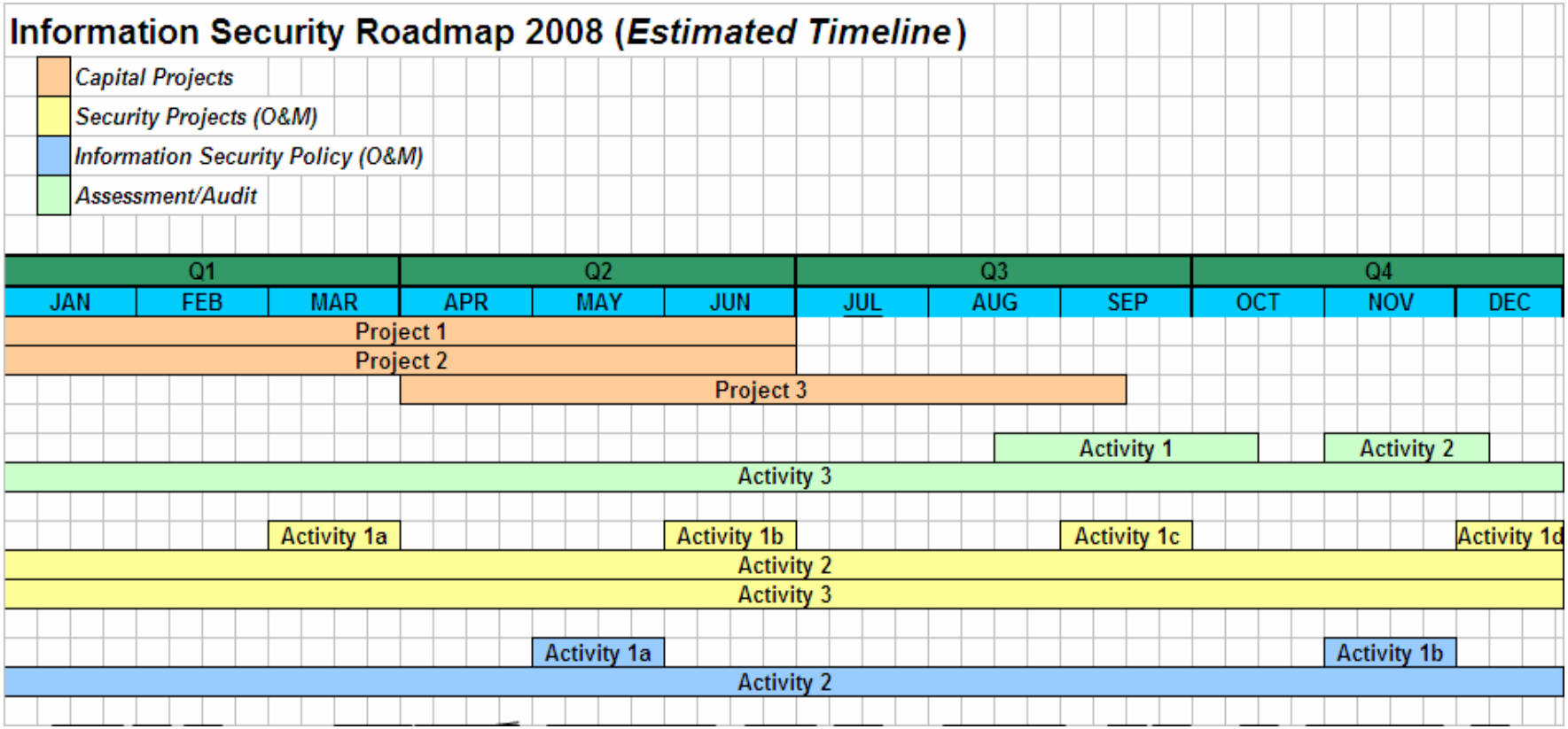
External:

- ERCOT Critical Infrastructure Protection Advisory Group (CIP-AG)
- NERC CIP Committee
- NERC CIP Task Forces and Drafting Teams
- ISO/RTO Security Working Group

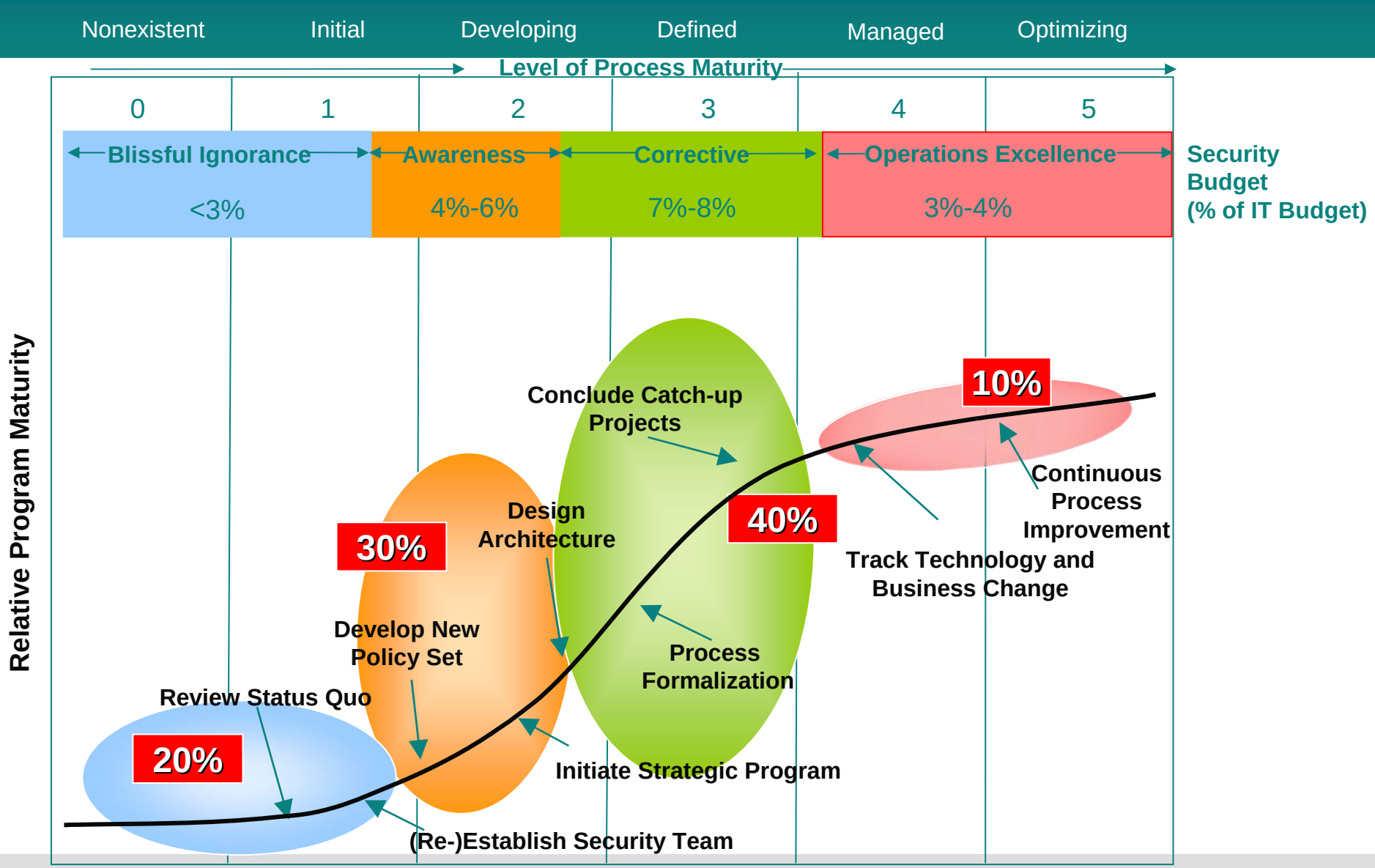
Internal:

- Corporate Security Advisory Group
- Line of Business Security Committee
- Security Risk Management Subcommittee

Information Security Roadmap



Security Program Maturity Timeline



NOTE: Population distributions represent typical, large G2000-type organizations

Source: Gartner

Thank You!