Cyber Standards Final Rule:
FERC Order 706

NERC Compliance Workshop
May 13, 2008

Jim Brenton, CISSP-ISSAP
Director, Security & CSO
ERCOT
jbrenton@ercot.com
512-248-3043

Scott Mix, CISSP
Manager of Situation Awareness
and Infrastructure Security, NERC
Scott.Mix@NERC.net
215-853-8204

Prerequisite Knowledge and Presentation Focus

- NERC CIP Stds 101: NERC "What" Workshop
  - ftp://www.nerc.com/pub/sys/all_updl/cip/owg/CSSET%20Workshop.zip
  - Dallas September 2006
- NERC CIP Stds 102: ERCOT "How-to" Workshop
  - http://www.ercot.com/calendar/2006/11/20061101-Cyber.html
  - Austin Met Ctr, November 2006
- NERC CIP Stds 201: FERC Order No 706
  - CIP 101/102 are prerequisites—available on line
  - Final FERC Rule No. 706 Highlights
  - NERC SAR and Standards Drafting Process
  - Implementation Schedule

Caveats / Notes FERC Order No. 706

- Not everything is captured in these notes
  - There are definitely additional issues in the Final Rule
- Not a substitute for review by each entity
- Not a comparison between the FERC NOPR and Final Order 706
- Red numbers (xx) following slide bullet points correspond to paragraph numbers in the FERC Cyber Security Final Rule:
  - **FERC Order No. 706**

Standards Development Timeline–Ancient History

- FERC Request to CIPAG, May 9, 2002
- "Security Standards for Electric Market Participants" transmitted to FERC on July 25, 2002
- FERC Publishes "Standard Market Design NOPR", with "Security Standards" as Appendix G on July 31, 2002
- SAR for UA1200 starts January 31, 2003
- UA1200 Standard Drafting begins March 11, 2003
- UA1200 adopted by industry vote June 27, 2003
- NERC Board Adopts UA1200 August 13, 2003
- UA1200 renewed by industry ballot on July 14, 2004 and July 29, 2005 (with Board re-approval following)
- UA1200 Replaced by CIP-002 – CIP-009 on June 1, 2006

Standards Development and Rulemaking Process

- SAR for Standard 1300 written May 2, 2003
- SAR approved on March 8, 2004
- Standards Drafting started June 8, 2004
- Cyber Security Std CIP002-1—CIP009-1 approved by industry on March 24, 2006
- Approved by NERC Board on May 2, 2006
- Submitted to FERC on August 28, 2006
- FERC Staff Report on December 12, 2006
- FERC NOPR issued on July 20, 2007
- FERC Final Rule issued on January 17, 2008
- Federal Register Notice February 7, 2008
- Effective Date 60 days* later (April 7, 2008)

"Final Rule" — FERC Order No. 706

- Final Commission ruling at Open Meeting on Jan 17
  - 72 weeks of deliberation, public comment, and rule writing after initial NERC submission to FERC
    - 104 weeks following last draft posting by NERC prior to balloting – "ballot draft"
  - 217 page order (single spaced)
    - NOPR was 197 pages (double spaced)
    - Staff Assessment was 44 pages (single spaced)
  - 70 sets of responses to NOPR
    - 38 sets of responses to FERC Staff Assessment
  - Final Order No. 706 may be found at

    http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf

Final Rule No. 706 Highlights

- Approve the eight Cyber Security Reliability Standards CIP002-1 thru CIP009-1 as submitted by NERC/ERO (13)
  - Approved without condition (27)
- FERC approved the Cyber Security Standards Implementation Plan as submitted (13)
- Existing (newly approved) CIP Standards to remain in effect until revisions are approved by the Commission (30)
- Not all NOPR proposals adopted in the Final Rule
  - Some adopted with modifications

Final Rule Highlights

- FERC directed modifications to CIP002-009 through existing NERC Standards Development Process (13)
  - Some guidance may in the form of examples (61)
  - Some guidance may be in the form of reference documents (61)
- Final Rule language is not prescriptive (28,29)
  - Alternative approaches to be considered, provided they address Commission's underlying concerns (29)
- Newly-directed modifications *DO NOT* affect the current Cyber Security Stds implementation plan (13)
  - Revised standards will have their own implementation plan (89)

General Issues

- Remove "Reasonable Business Judgment" language (128)
  - Acknowledge importance of flexibility and discretion (131)
  - Standards Development Process may propose alternative language (135)
  - Remove before compliance audits begin (138)
- Remove "Acceptance of Risk" language (150)
  - Proposed that alternative language tying result to technical feasibility is preferable (151)

General Issues

- Modify "Technical Feasibility" language (178)
  - Adapted to encompass a broader range of technical justification (move from "acceptance of risk" to "technical feasibility") (151)
  - Not based in "Reasonable Business Judgment" language (178)
  - Includes "technically safe" and "operationally reasonable" (182)
  - Requirement to develop a mitigation plan that includes remediation plan or compensating measures, and timeline to eliminate "technical feasibility" exemption (192)
    - No requirement for "date certain" for removal of exemption (192)
    - Explanation of why no reasonable completion date in plan (192)

General Issues

- Modify "technical feasibility" language (cont'd)
  - Approval of exception reports by Senior Management (211)
  - Regional Entity and ERO to provide oversight through audit process (and on-site inspection to reduce amount of sensitive information removed from responsible entity) (213, 214)
  - Earlier scheduling of audits based on number of "technical feasibility" exceptions claimed by an entity (215)
  - Regional Entity/ERO to approve "technical feasibility" exceptions during audits (218)
  - Addressed CEII and FOIA concerns about exception report data (219)

General Issues

- Future modifications would not overlap NERC implementation plan (26,87)
  - However, modifications to be be done in parallel with existing implementation plan (88, 89)
- If a directed modification implies a specific outcome, ERO may alternatively address the underlying issue through the Standards Development Process (29)
  - Equivalent alternative approaches require demonstration that they address the underlying Commission concern. (29)

General Issues

- Concept of "mutual distrust" (33)
- NERC registration process is appropriate for identifying who must comply (49)
  - Registration process will identify applicable entities based on their impact to reliable operations, e.g., a blackstart unit, regardless of size or connection voltage (50)
- Demand-side aggregators should be registered (51)
- Third-party suppliers – responsible entity remains responsible (52)
  - Contractual obligation (52)
  - Address in required policy (53)
  - No excuse allowed for 'off-shore' contracted entities

General Issues

- Guidance
  - Additional guidance could be in the form of examples (61)
  - In some cases, guidance must be placed in the standard itself (61, 62)
    - Oversight
    - Exceptions
    - Reports to Commission
  - Other cases, guidance may be in a supplemental document (61)
- Audits are only one aspect of ERO compliance (63)
  - Other aspects also required (63)

General Issues

- Compliance is to Requirements, not to Measures (72)
  - Failure to maintain documentation, as described in the measure, that obstructs the ability of the ERO to determine compliance with the Requirement may warrant a penalty (73)
- Include explicit requirement to implement a developed plan, procedure, etc (75)
  - Deviation from plans requires documented justification (76)

General Issues

- Require semi-annual self-certification prior to full compliance date (96)
- ERO and regions expected to provide informational guidance upon request (97)
- NIST Guidance not required (232)
  - Consider applicable features of NIST risk management framework in future revisions (233)
  - NERC to consult with Federal Agencies to evaluate effectiveness of NIST Guidance and CIP standards and report to Commission (233)
  - Commission may revisit the issue in the future (233)

CIP-002 – Critical Cyber Asset Identification

- ERO to provide additional guidance regarding risk-based assessment methodology (253)
  - Either as standards requirements or separate guidance documents (253)
  - Provide wide-area impact analysis – either ERO/Region or a designated entity (e.g., RC) (255)
- Scope of Critical Assets and Critical Cyber Assets (270)
  - Data (but not "marketing or other data") (270, 272)
  - Control Systems (279)
    - Misuse of systems (280, 281, 282)
  - No change in "non-routable protocol" use (285)
  - No requirement to justify why an asset was chosen or not (288)

CIP-002 – Critical Cyber Asset Identification

- Internal management review of methodology (294)
  - Senior manager annual approval of methodology in addition to results (294)
  - Consider changing "senior manager" to "officer or equivalent" (296)
- External review of Critical Asset Lists (319)
  - ERO to develop changes to standards (possibly assign responsibility to RCs) (328)
  - Regional Entities maintain oversight responsibilities (328)
  - Confidentiality concerns (330-334)
- Interdependency to Other Infrastructures (340)
  - Not addressed (341)

CIP-003 – Security Management Controls

- Adequacy of policy guidance (355)
  - Additional guidance (but not necessarily in the standard) (355)
- Discretion to grant exceptions (372)
  - Oversight of exceptions through existing audit process (272)
- Leadership (381)
  - Single manager (381)
- Information Access authorization (386)
  - Interlink CIP-003, CIP-004, CIP-007 (386)
  - 'Prompt' revocation of access when warranted (386)
    - No distinction between 'for cause' or 'friendly' termination (386)
    - "As soon as possible but no later than 24 hours from time of termination for cause" (386)

CIP-003 – Security Management Controls

- Change control and configuration management (397)
  - Express consideration of accidental consequences and malicious actions along with intentional changes (397)
- Interconnected networks (407)
  - Guidance on concept of "mutual distrust" (408, 409)

CIP-004 – Personnel and Training

- Training (431)
  - Train before access, but with limited exceptions for emergencies (431)
  - Escort allowed for new-hires prior to training (432)
  - Consider core training elements (433)
- Personnel risk assessments (443)
  - Check before access, but with limited exceptions for emergencies (443)
  - Discretion in who is allowed to review PRA results (446)

CIP-004 – Personnel and Training

- Cyber and physical access (460)
  - "Immediate" revocation of access in all cases (460)
  - ERO to define what circumstances justify an exception to the immediate requirement, and determine what is the fastest revocation possible (462)
- Jointly owned facilities (473)
  - All joint owners are responsible for protection (473)
  - If one owner declares the asset critical, all owners must treat it so (?) (473)
  - Joint owners perform assessments of their own personnel (474)

CIP-005 – Electronic Security Perimeters

- Adequacy of Electronic Security Perimeters (496)
  - "Implement two or more defensive measures in a defense in depth posture" (496)
  - Technical feasibility exemption allowed (496)
- Protecting access points and controls (511)
  - Provide examples of "strong authentication" (511)

CIP-005 – Electronic Security Perimeters

- Monitoring access logs (525)
  - Review logs more frequently than 90 days, but not necessarily daily (525)
  - Manual review even where automated tools implemented (526)
  - Statistical sampling of reviewed logs (528)
- Vulnerability assessments (541)
  - Adopt ERO proposal of "active", rather than "live", vulnerability assessments every three years, or upon significant change (541-545)
  - Annual "paper" assessments in intervening years (545)

CIP-006 – Physical Security

- Physical Security Plan (559)
  - Treat "alternative measures" as "non-interim" technical feasibility exceptions (560)
- Physical Access controls and monitoring (572)
  - "Implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets" (572)
  - Technical feasibility exemption allowed (572)
- Maintenance and Testing (581)
  - Test more often than every three years (581)

CIP-007 – System Security Management

- Acceptance of risk and technical feasibility (597)
  - Eliminate "acceptance of risk" terminology; "technical feasibility" remains subject to previous discussion (597, 600)
- Test procedures (609)
  - Address what constitutes a "representative system" (609)
  - Document differences between production and test, but not document mitigations taken due to differences (609)
- Malicious Software Prevention (619)
  - Includes safeguards against introduction of malicious code by personnel (621)

CIP-007 – System Security Management

- Security status monitoring (628)
  - Review logs more often than 90 days (628)
  - Manual review even where automated tools implemented (629)
  - Statistical sampling of reviewed logs (629)
- Disposal or redeployment (633)
  - Disposal and redeployment are different (633)
  - Clarify "prevent unauthorized retrieval of data" (634, 635)
  - Note that Commission believes that DoD "7 pass" overwrite is insufficient for disposal (??) (633)

CIP-007 – System Security Management

- Cyber Vulnerability assessment (643)
  - Provide direction on "what features, functionality, and vulnerabilities" are needed for a vulnerability assessment (643)
  - Entity-imposed timeline for completion of action plan (643)
- Documentation review and maintenance (651)
  - Update documents in less than 90 days (651)
  - Suggests 30 days with exceptions granted for extraordinary circumstances (651)
  - Clock starts upon final implementation of modification (652)

CIP-008 – Incident Reporting & Response Planning

- Definition of reportable incident (660)
  - Provide guidance on definition (660)
  - Breaches may occur through physical or cyber means (661)
  - Harmonize term with other references (e.g., DOE-417) (661)
  - Not triggered by Internet noise attacks (661)
  - Resulting language can be audited and enforced (661)

CIP-008 – Incident Reporting & Response Planning

- Reporting (673)
  - Report as soon as possible, but within one hour of discovery of incident (673)
  - Report to "appropriate government authorities" and "industry participants" (675)
  - Preliminary report required during recovery activities; full (final) report once system is restored (674)
- Full operational exercises and lessons learned (686)
  - Maintain documentation of drills and actual incident responses (686)
  - Require revisions to incident response plans to address lessons learned (686)
  - No requirement to remove equipment from service (687)
  - Alternative term acceptable (687)

CIP-009 – Recovery Plans

- Recovery plans (694)
  - Recovery plans required (694)
  - Failure to implement recovery plans results in non-compliance (694)
- Forensic data collection (706)
  - Did not imply criminal proceeding rigor for "forensics" (707)
  - Allows ERO phrase "data collection for post-event analysis, where technically feasible" (709)
  - Preserving evidence should not hinder system restoration (708)

CIP-009 – Recovery Plans

- Operational exercises (725)
  - Require "operational exercise" (not "full operational exercise") every 3 years with table-top exercises annually in other years (725)
  - Demonstrated recovery in representative test environments (725)
- Updating recovery plans (731)
  - Update plans more rapidly than 90 days (731)
- Backup and storage of restoration data (739)
  - "Test" prior to storage (739)
  - Create backup following "significant changes" (740)
- Testing of backup media (748)
  - Ensure backups are successful and backup failures are addressed (748)

Violation Risk Factors – VRFs

- Revised ERO filing due 90 days before the standards become enforceable (757)
- 162 VRF's accepted as submitted
- See NOPR for specific table of requirements (NOPR)
- Supply missing VRFs for 9 requirements
- Revise 43 VRFs as identified in NOPR (767)
  - All modifications are "up" (NOPR)
  - Specifically: CIP-002 R2 & R3 from Medium to High (761, 762)

Guidelines

- Some of the guidelines topics may also have associated changes to standards requirements
- Some guidelines have been started as part of planned CY2008 Working Group plans
- However, not all guideline recommendations are "within scope" of a current Working Group plans

Guidelines – Already Started

- Guidelines Already Started:
  - Risk-based Assessment Methodologies (237-288)
  - Reporting timeframes, thresholds and criteria (660, 674)
- Security Policy topics and processes (355)
  - Power supplies, heating, other equipment (358)
- Additional topics for securing critical cyber Assets (356)
- Communications from common carriers (360)
- Mutual Distrust (408, 412)

New Guidelines to Be Developed

- Background checks (466) [may also include changes to the standard]
- Defense in depth – electronic (502)
- Strong Authentication (511)
- Verification Technologies (511)
- Log review – "readily accessible logs" (527)
- Vulnerability Assessments (547)
- Defense in depth – physical (575)

New Guidelines to Be Developed

- Physical security testing – "readily accessible facility" (581)
- Testing (582)
- Representative systems for testing (609)
- Confidentiality in reviewing assessments (guidance to teams) (612)
- Introduction of malicious code and viruses (621)
- Log sampling (629)
- Vulnerability assessments (644)

New Guidelines to Be Developed

- "Full Operation Exercise" or alternate term (687)
- "Demonstrated recovery" concept (725)
- Backup, restoration, backup testing, etc (739)

Semi-Annual Survey

- FERC has directed semi-annual surveys of each Registered Entity's progress toward reaching the "Compliant" stage of the CIP Implementation Plan

- If a Registered Entity indicates they have not yet reached the "Compliant" milestone for a requirement, the Registered Entity will be required to file a Remedial Action Plan.

  There are no sanctions or penalties

- Expect the Semi-Annual Surveys to commence August 1st and February 1st, starting August 1, 2008

  Final details under review and pending

Compliant Stage

- "Compliant" means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records"

- After the Compliant date, Registered Entities are subject to the CMEP process which includes Remedial Action Plans, Sanctions and Penalties

Compliant Stage – Monitoring Methods

- **Self-Reporting** – Registered Entity is to report when they are not "Compliant" or "Audibility Compliant" with a requirement

- **Self-Certification** – Begins July 1, 2008 with first survey reports due August 1 – More details to follow
  - The Self-Certification process will be managed so that the Self-Certification is sent to the Registered Entity by the Regional Entities within the agreed upon time frame.

- **Investigations** – For cause due to an event, complaint, report or by other means

NERC Standards Action

- Standards Authorization Request (SAR) Process was initiated to implement FERC changes
  - "Implement Changes to the … Cyber Security Standards as indicated in FERC Order 706"
  - Submitted for Standards Committee (SC) for consideration at their 3/10 meeting
- SC Approved SAR on 3/11 with "Minor Changes"
- SAR posted for stakeholder review and available at: http://www.nerc.com/%7Efilez/standards/Project_2008-06_Cyber_Security.html
  - Nominations for SAR Drafting team members through April 4
  - Solicited comments on SAR through April 19

Next Steps

- SAR Drafting Team
  - Call for SAR Drafting Team volunteers in March
  - Drafting Team appointed by SAC, NOT CIPC—over 70 applicants for 15 slots
  - "Others" may participate in SAR Drafting Process but may not vote as members
- Some initial changes to standards may be drafted and posted for comment in parallel with SAR Development
  - Non-controversial, "low hanging fruit", e.g., Sr. Manager approval of risk-based assessment methodology
  - Items that appear to be controversial may be removed prior to ballot
- Some groups have filed exceptions to this approach—results are TBD

Next Steps

- Standards Drafting Team(s)
  - Probably, multiple iterations, multiple timelines, multiple teams?
    - Simple and easy first, then harder issues
    - Work in parallel, but move toward ballot quickly
    - Will probably result in multiple "versions" of the standards sent to BOT and Commission
  - However, some groups requesting one team that focuses on one version, not multiple versions—TBD

Next Steps

- Standards Drafting Team(s)
  - Others groups have requested one implementation schedule, not multiple versions
  - What about newly declared Critical Assets and CCAs—when does the Responsible Entity have to bring the CCAs into compliance?
    - Immediately or over some multi-year transition plan?
  - Should entities with internal security measures that exceed the CIP requirements be held responsible for compliance with their internal measures or with the less stringent NERC measures.

References

- Urgent Action 1200
  - http://www.nerc.com/~filez/standards/Cyber_Sec_Renewal.html
- NERC Standards CIP-002 through CIP-009
  - http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection
- Frequently Asked Questions
  - ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf
- Implementation Plan
  - ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Revised_Implementation_Plan_CIP-002-009.pdf

References

- Archive of draft postings and comments
  - http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html
- "What" Workshop presentation files
  - ftp://www.nerc.com/pub/sys/all_updl/cip/owg/CSSET%20Workshop.zip

References

- FERC Staff Assessment of CIP Standards
  - http://www.ferc.gov/industries/electric/indus-act/reliability/12-11-06-cip.pdf
- NERC Response to Staff Assessment
  - ftp://www.nerc.com/pub/sys/all_updl/docs/ferc/RM06-22.pdf
- FERC NOPR on CIP Standards
  - ftp://www.nerc.com/pub/sys/all_updl/docs/ferc/CIP_NOPR.pdf
- NERC Response to NOPR
  - ftp://ftp.nerc.com/pub/sys/all_updl/docs/ferc/FiledCyberOct5.pdf

References

- FERC Final Rule – Order 706
  - http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf
- SAR for "Version 2" (proposed)
  - ftp://ftp.nerc.com/pub/sys/all_updl/standards/sc/SC_10-11Mar08_Agenda.pdf (attachment 4d)

Questions

Scott.Mix@NERC.net
215-853-8204

jbrenton@ercot.com
512-248-3043

NERC Sanction Guidelines

- Base Penalty determined by two criteria…
  1. **Violation Risk Factor** assigned to each requirement
     - Lower, medium, or high risk
  2. **Severity of the Violation** (level of noncompliance)
     - Lower, moderate, high, or severe

- Adjustments to base penalty
  - **Violator size/ability to pay and actual impact violation on system reliability**
  - **Reward –** Unsolicited self-reporting, quality internal compliance programs, voluntary corrective actions, etc.
  - **Punish –** Repeat violation, evasion, inaction, unwarranted intentional violations (e.g., economic choice), etc.

NERC Sanction Guidelines

- Adjustments to base penalty
  - **Aggravating factors** – increase penalty
    - Repetitive infractions & prior warnings
    - Deliberate violation
    - Lack of cooperation
  - **Mitigating Factors** – reduce or minimize penalty
    - Prompt disclosure
    - Voluntary and prompt corrective actions
    - Substantial cooperation
    - Quality of compliance program and overall performance

However, "No penalty is to be inconsequential"

(David Whiteley, Executive VP, NERC)

Penalty Matrix

Violation Risk Factor	Violation Severity Level							
	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

* FERC statutory limit: $1,000,000 per day--this matrix is still undergoing revision

Reliability Audits

- Reliability Audits - focuses on "did the entity meet the requirement?" Yes/No
  - Sanction will be assessed for compliance violations
  - Sanction amount based on Base Penalty Amount plus Adjustments

- ERCOT ISO planning for an "audit" or "evaluation" of Cyber Security Standards implementation after effective date of July 1, 2008
  - ERCOT ISO (RC/BA/TOP) was subject to UA-1200 Self-Certification
  - Table 1a of the NERC Implementation Plan applies

Compliance Implementation Schedule

Date	Substantially Compliant Stage	Compliant Stage	Auditably Compliant Stage
7/1/2008	28 Requirements	13 Requirements	
7/1/2009		28 Requirements	13 Requirements
7/1/2010			41 Requirements

ERCOT Information Security Strategy

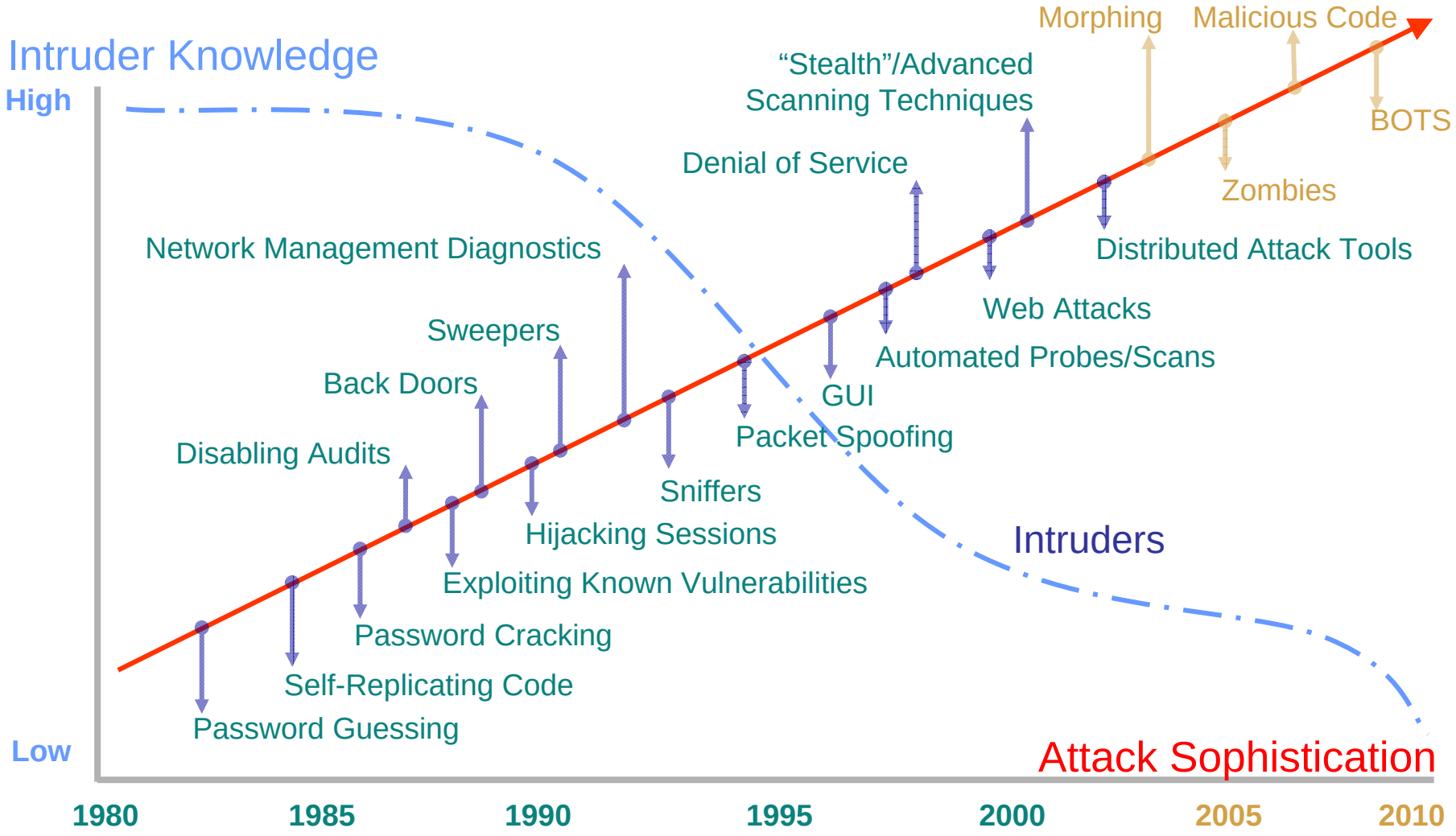
Ann Delenela, CISSP CISM

Information Systems Security Manager

Overview

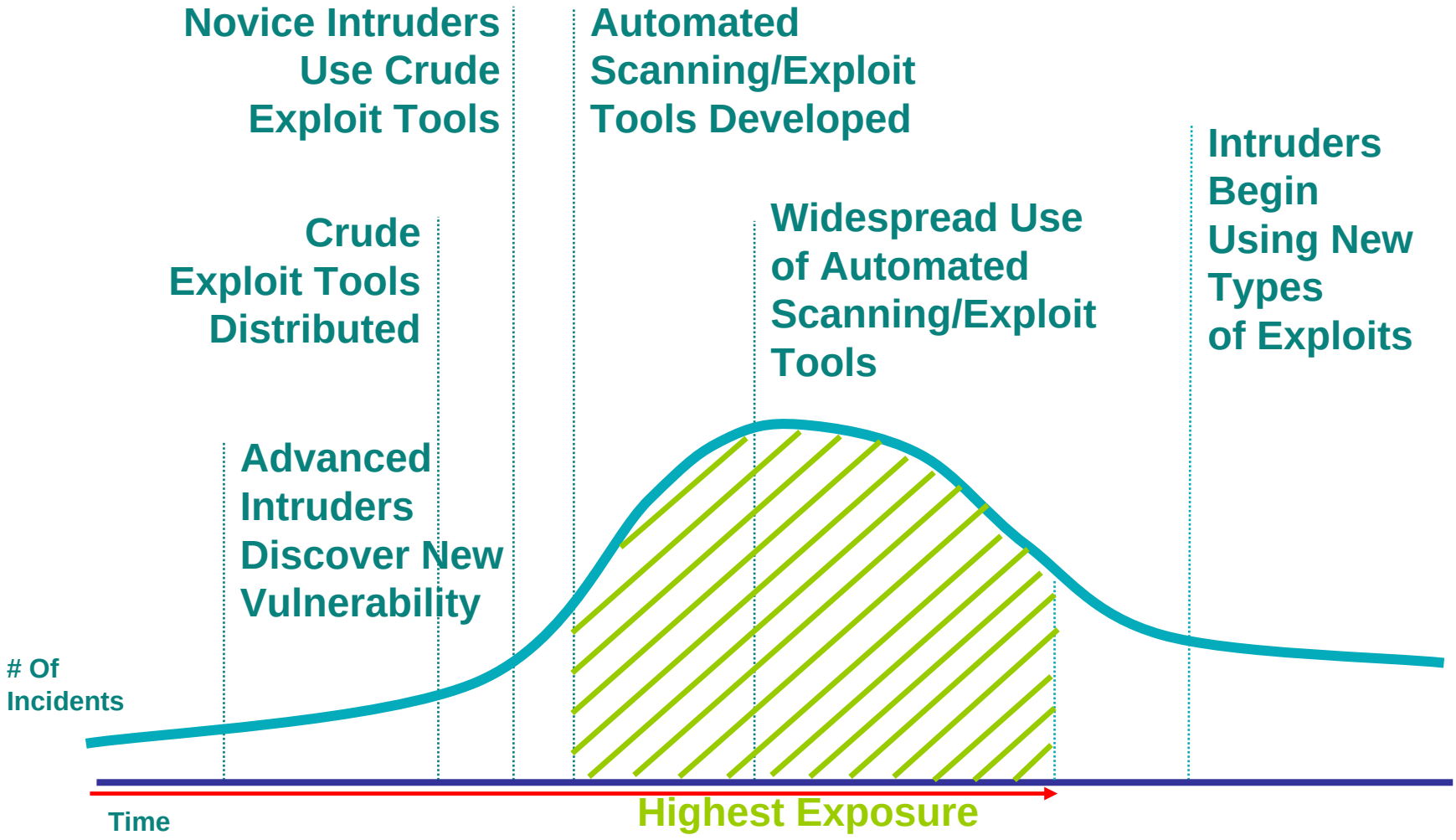
- Threats & Vulnerabilities
- Security Management Framework
- Protection Strategy
- ERCOT Information Security Mission Statement & Organization
- Information Security Roadmap
- Security Maturity Model

Attack Sophistication vs. Intruder Knowledge



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

Vulnerability Exploit Cycle



Source: Federal Bureau of Investigation

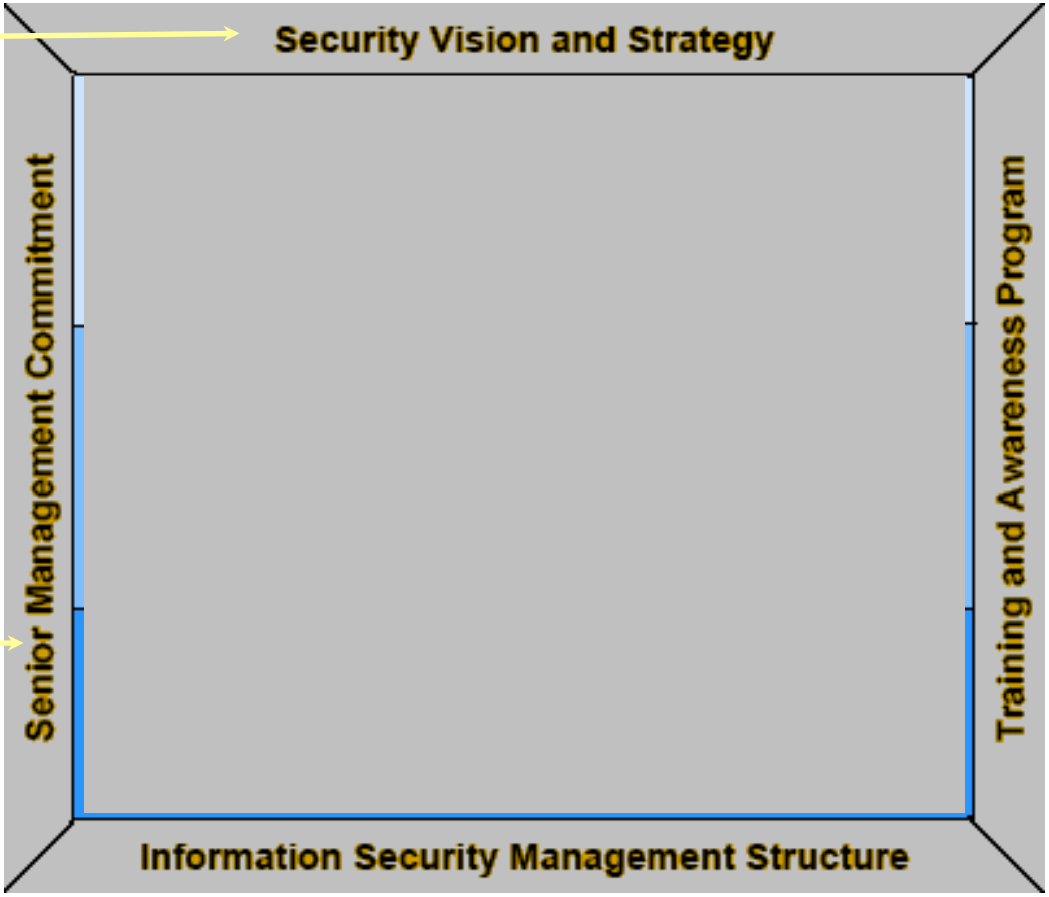
Information Security Management Framework

1) Security Vision & Strategy:

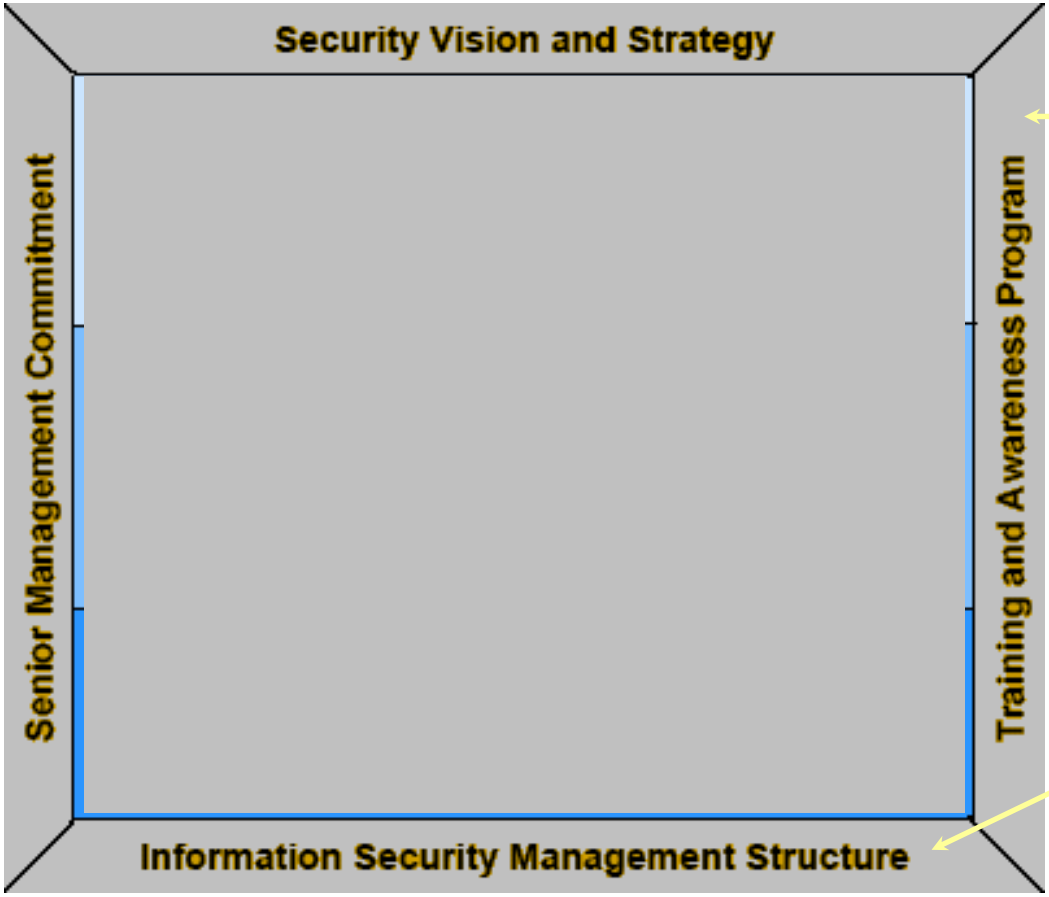
- Mission Statement, guiding principles
- Strategy for addressing information protection
- Security/Executive committee as an authoritative decision & communication vehicle

2) Sr. Mgmt Commitment:

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



Information Security Management Framework



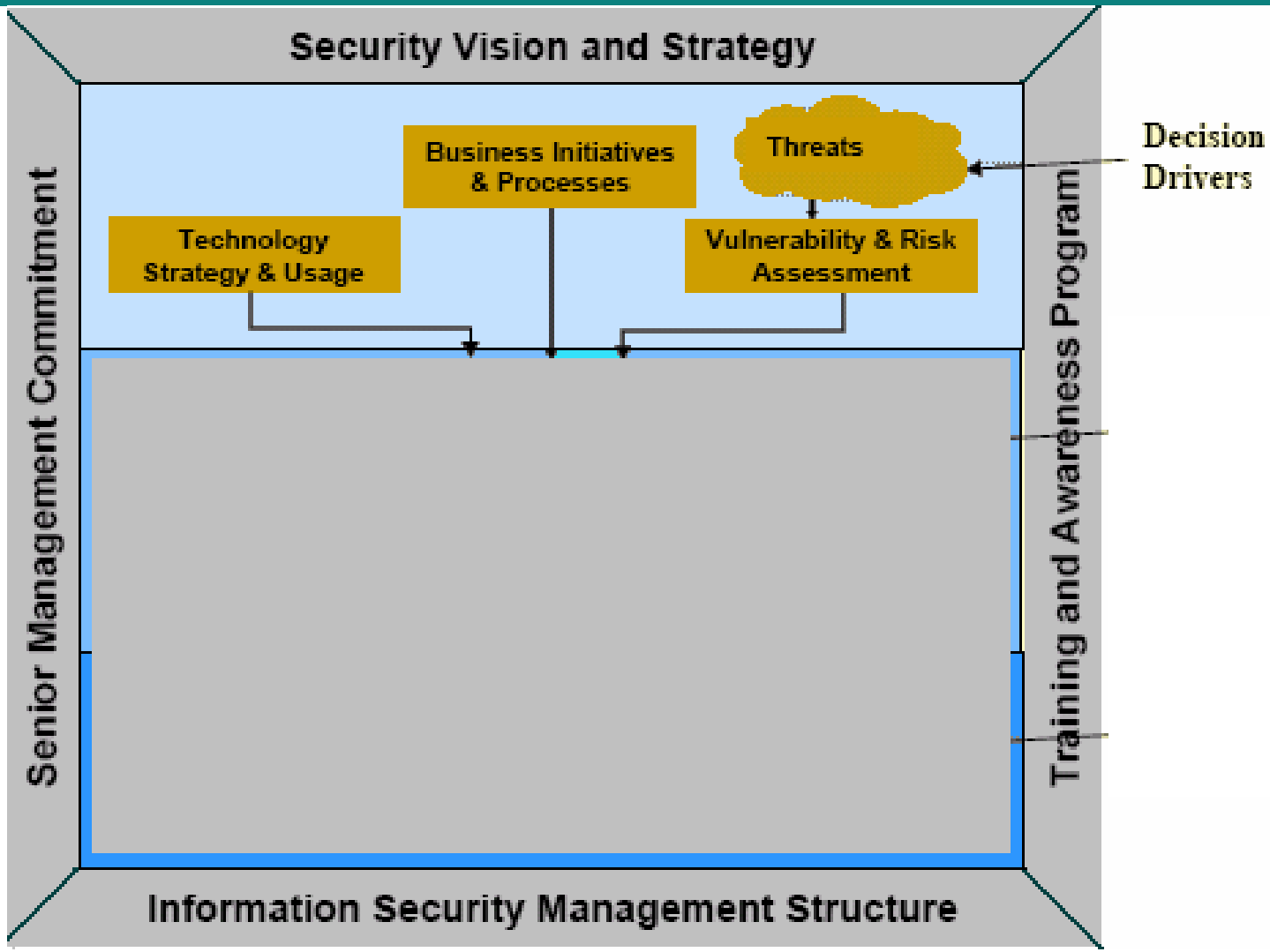
4) Training & Awareness Program:

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

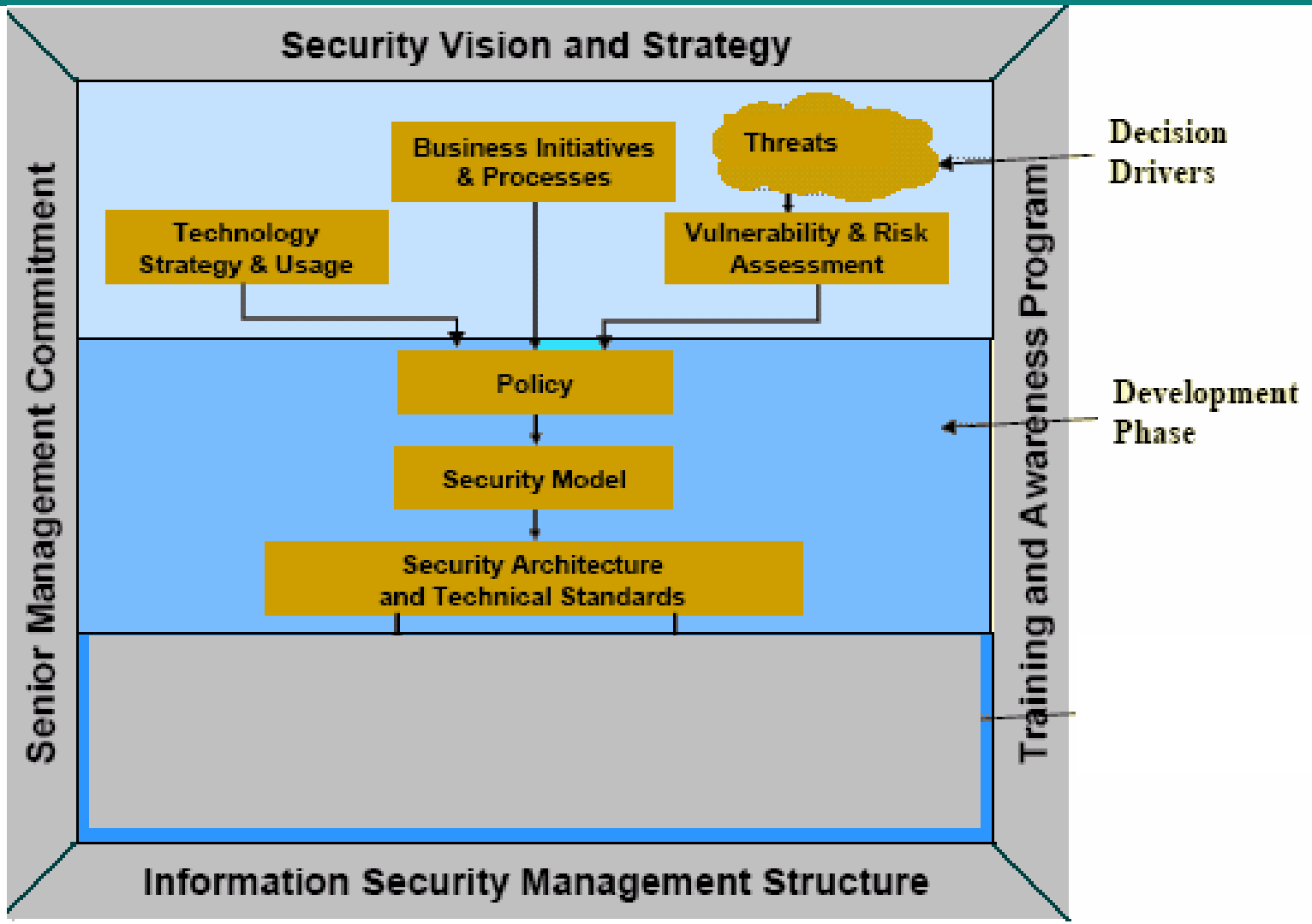
3) Security Mgmt Structure:

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

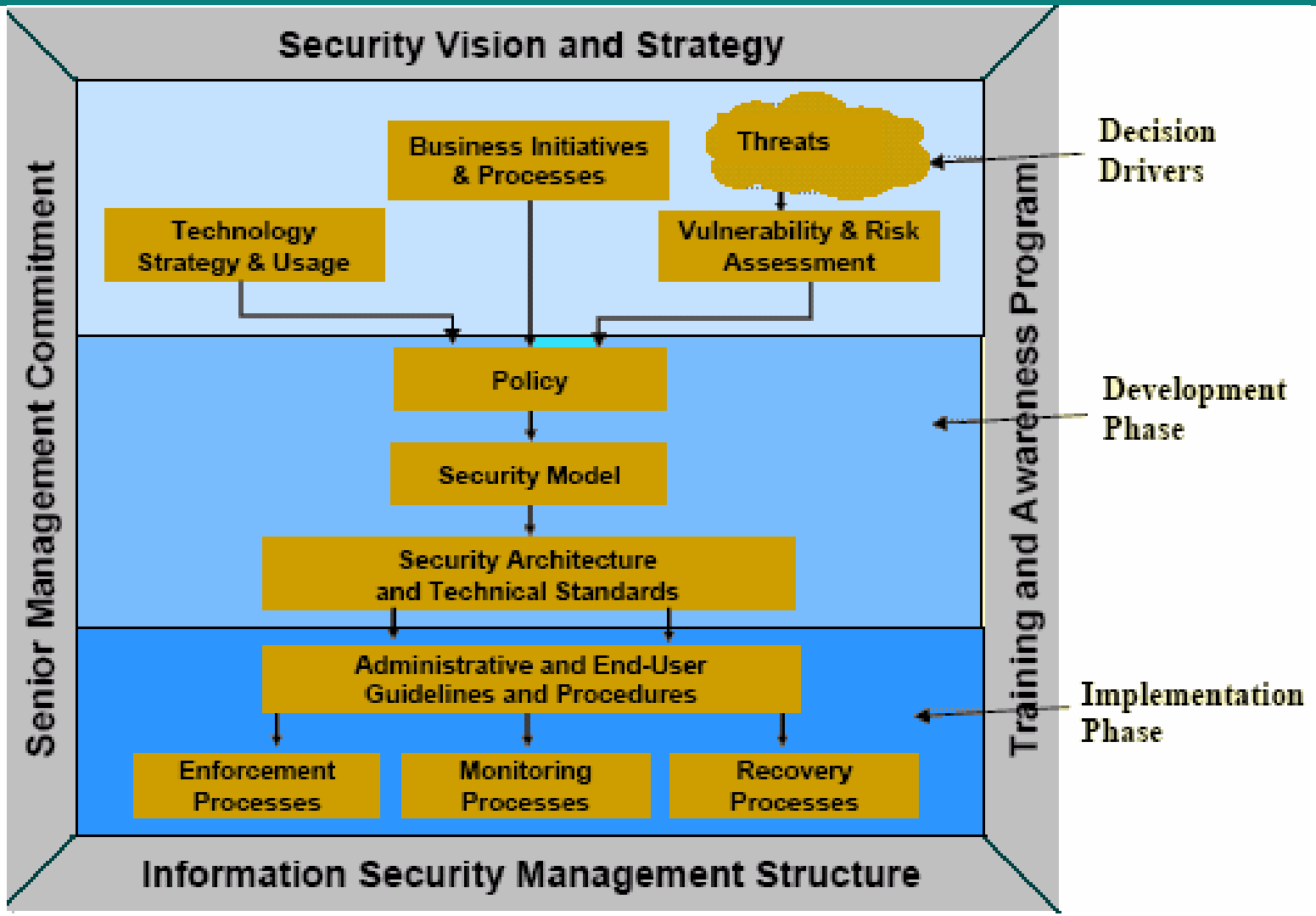
Information Security Management Framework



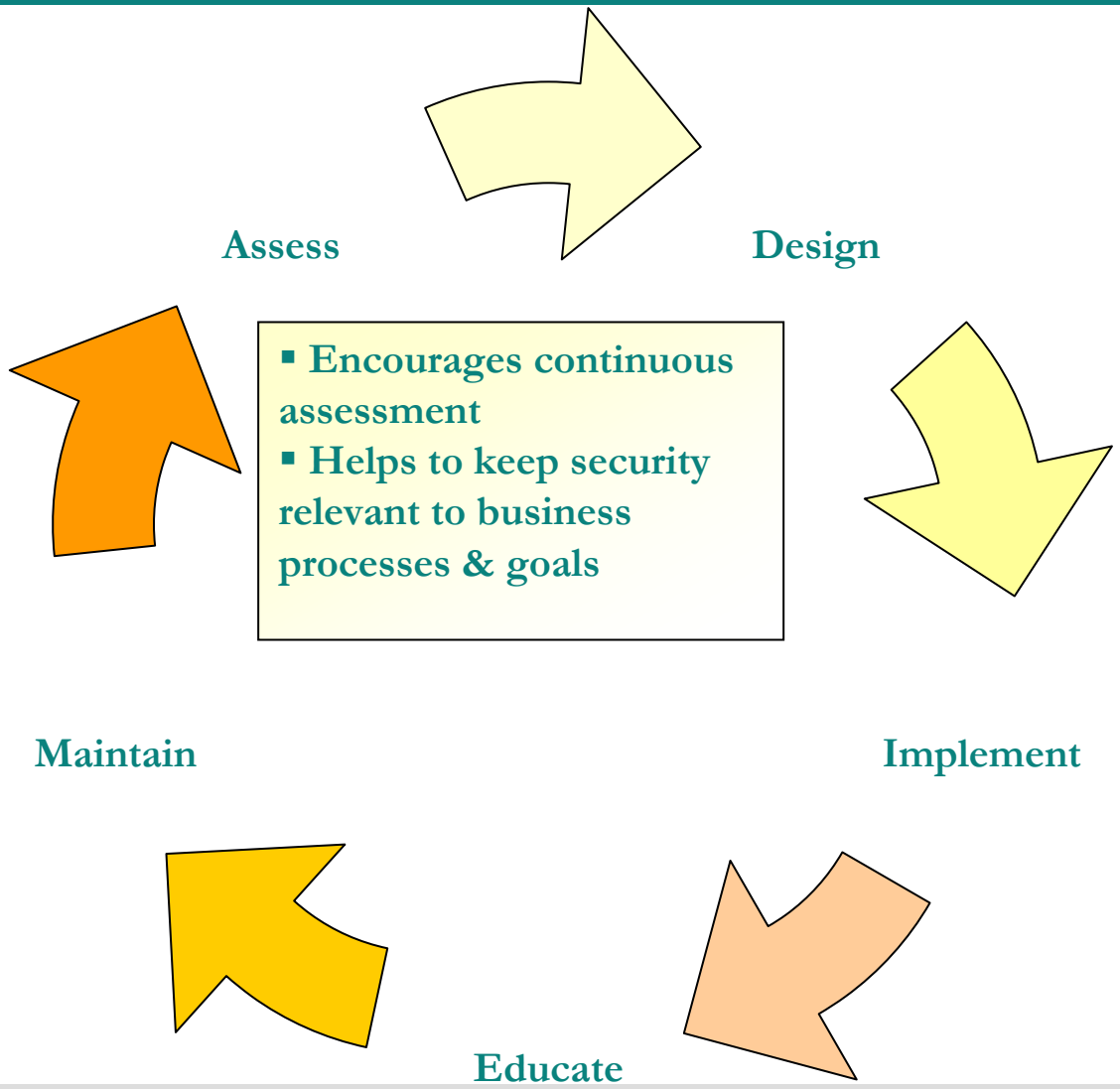
Information Security Management Framework



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

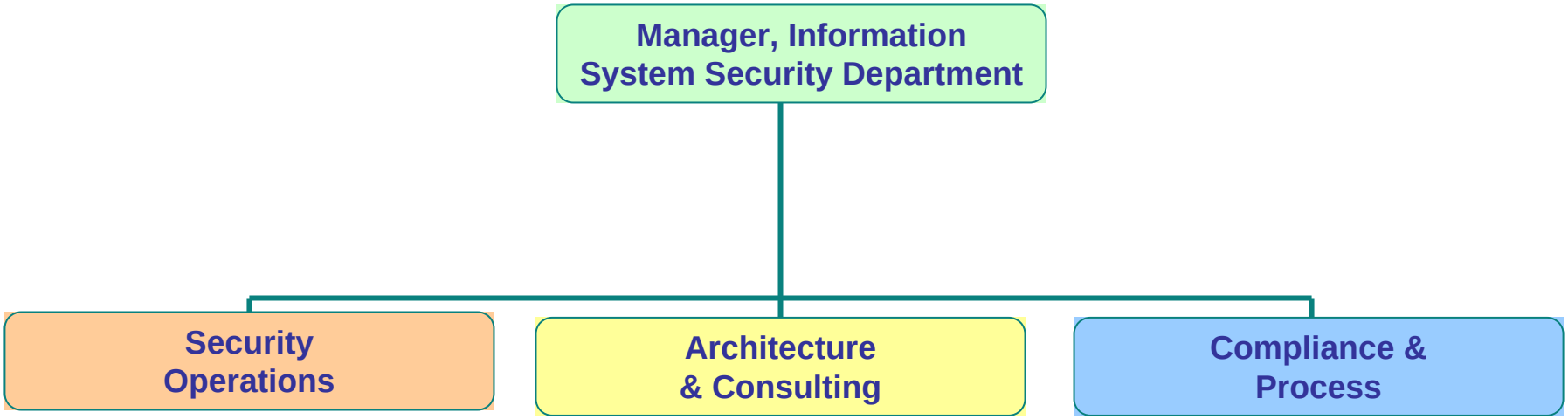
ISSD Mission Statement

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

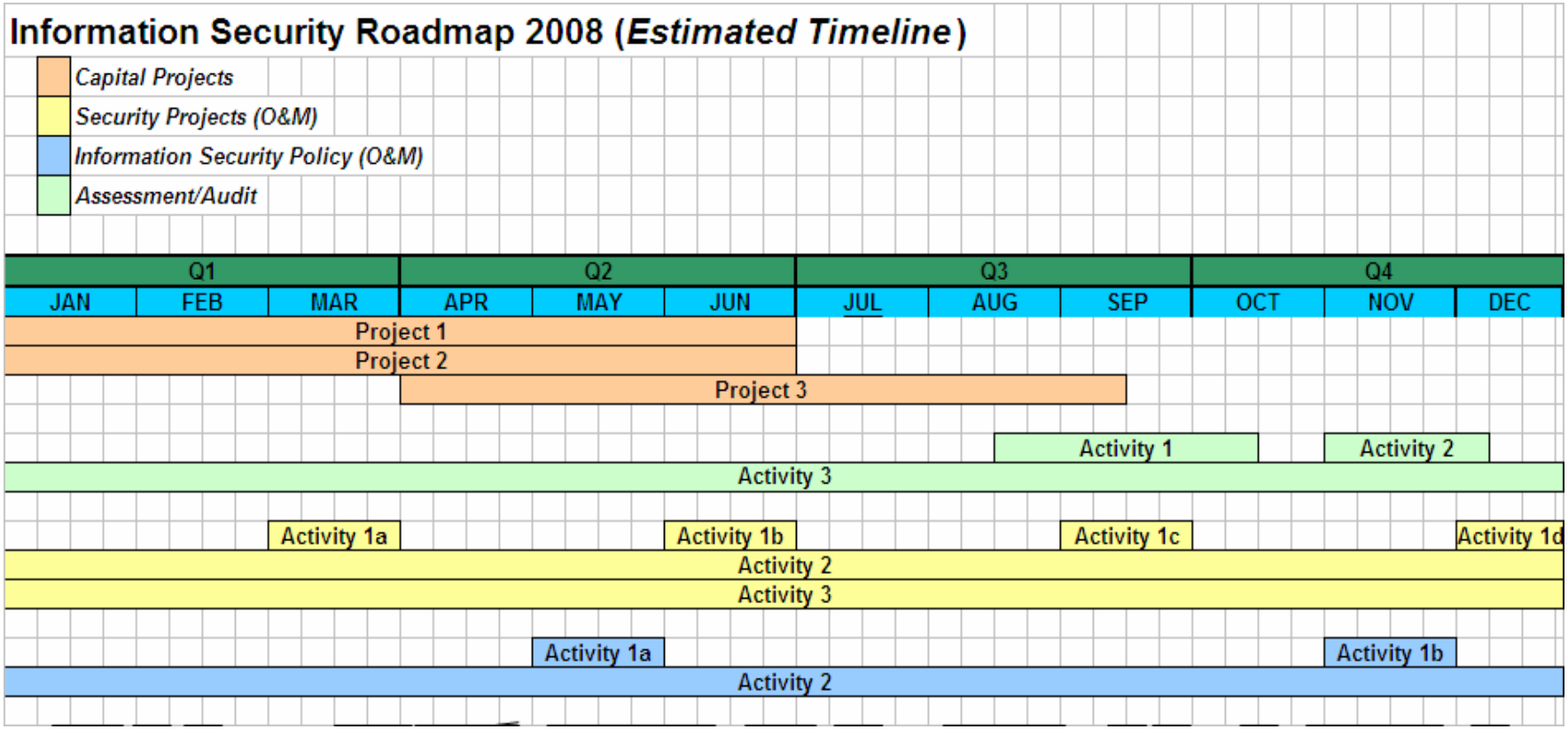
External:

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

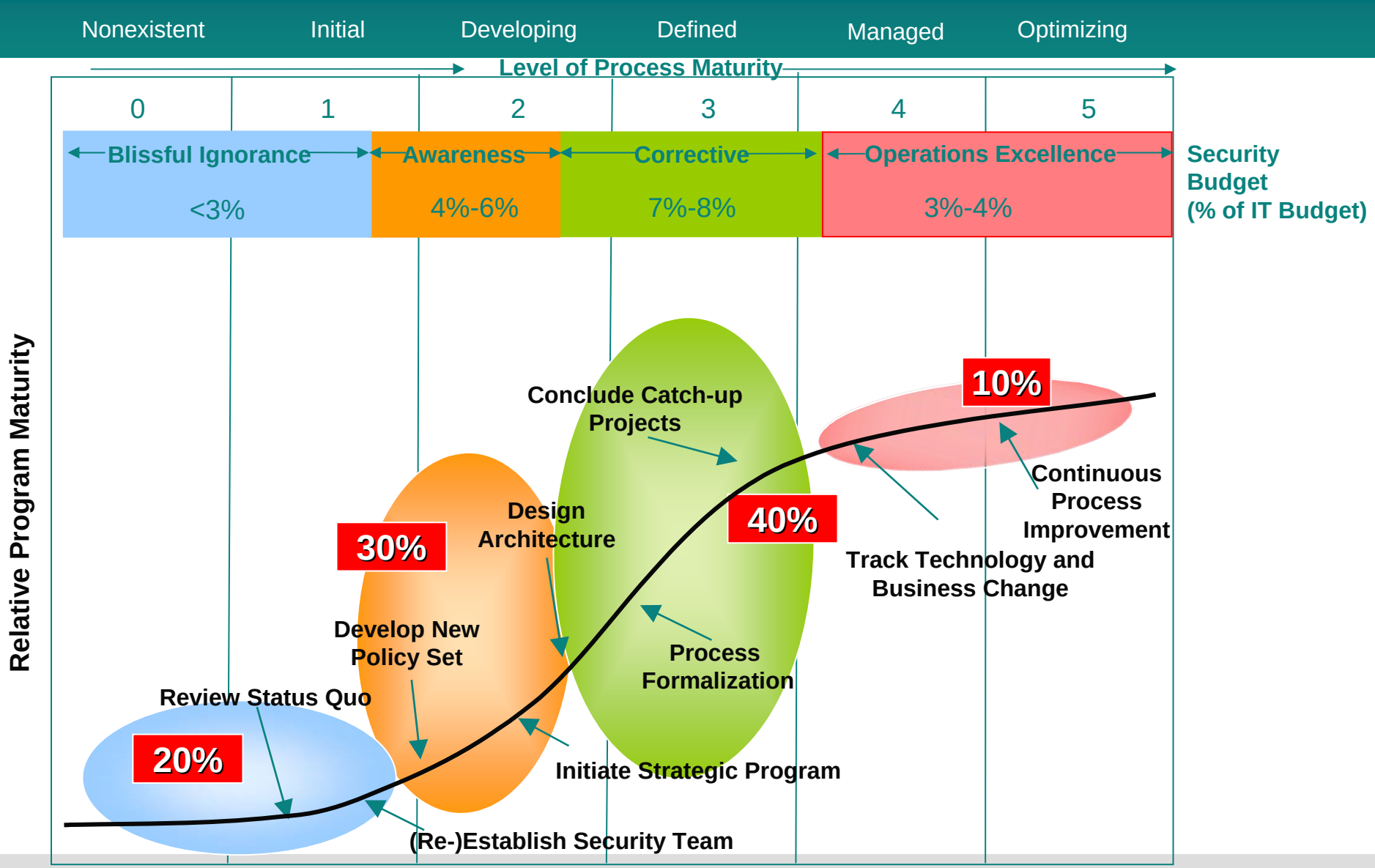
Internal:

- 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!