

Security Programs and Regulatory Compliance

Patrick C Miller, CISSP SSCP IAM TCP
IPMA Forum 2004 – St. Martin's College, Lacey, WA
May 25th, 2004



Information Security

is a dynamic, constantly evolving, living system. Breakwater keeps ahead of the curve and anticipates threats to provide clients with highly responsive protection.



Presentation Overview

- **Breakwater Profile**
- **Current Situation**
- **Regulatory Landscape**
- **Security Program Roadmap**
- **Metrics and Framework**
- **E-Government Solutions**
- **Resources**

Interaction is encouraged...



Breakwater Security Associates

Information Security and Risk Management Services Firm since 1996.

A few of the things we do well...

- **Security Program Development**
 - Risk, Security and Vulnerability Assessments
 - Regulatory Compliance Gap Analysis
 - Policy Development and Auditing
 - Security Strategy
- **Managed Security Services**
 - Device Management
 - Event Correlation (Security Risk Management)
 - Monitoring
- **Training/Education**
- **Integration**



The Current Situation...

- Information Crime
 - Corporate Accountability (Enron, WorldCom, etc...)
 - Id Fraud
- Weak Economy
 - Fewer jobs overall
 - Pink slips = increased workload, frustration and disgruntled employees
- Technology Shift
 - Automation (Process Control Systems); doing more with less
 - Ever-increasing complexity and power
- e-Government
 - Need for access to Internal Applications
 - Not all departments are ready for this; classification nightmare
- Terrorism
 - Can they use our people, processes, or technology against us?
- Lack of Expertise and Experience
 - Talent is scarce and “snake oil” is common



The Regulatory Landscape

All of this means that more regulations are coming and we are only seeing the tip of the iceberg...



Regulatory Avalanche

Why all the new regulations?

- The current situation...
- Most organizations **are not** implementing good security; many reasons for this
- Disagreement on what “good security” actually is or should be by industry working groups
- Unclear or lack of visibility into security within organizations by regulatory agencies
- Competing security standards that overlap or even conflict; very little coordination or centralization
- Industry self-regulation is getting bad press for not moving fast enough
- Technology has altered the risks; good timing
- *The Department of Homeland Security (DHS) is just getting started...*

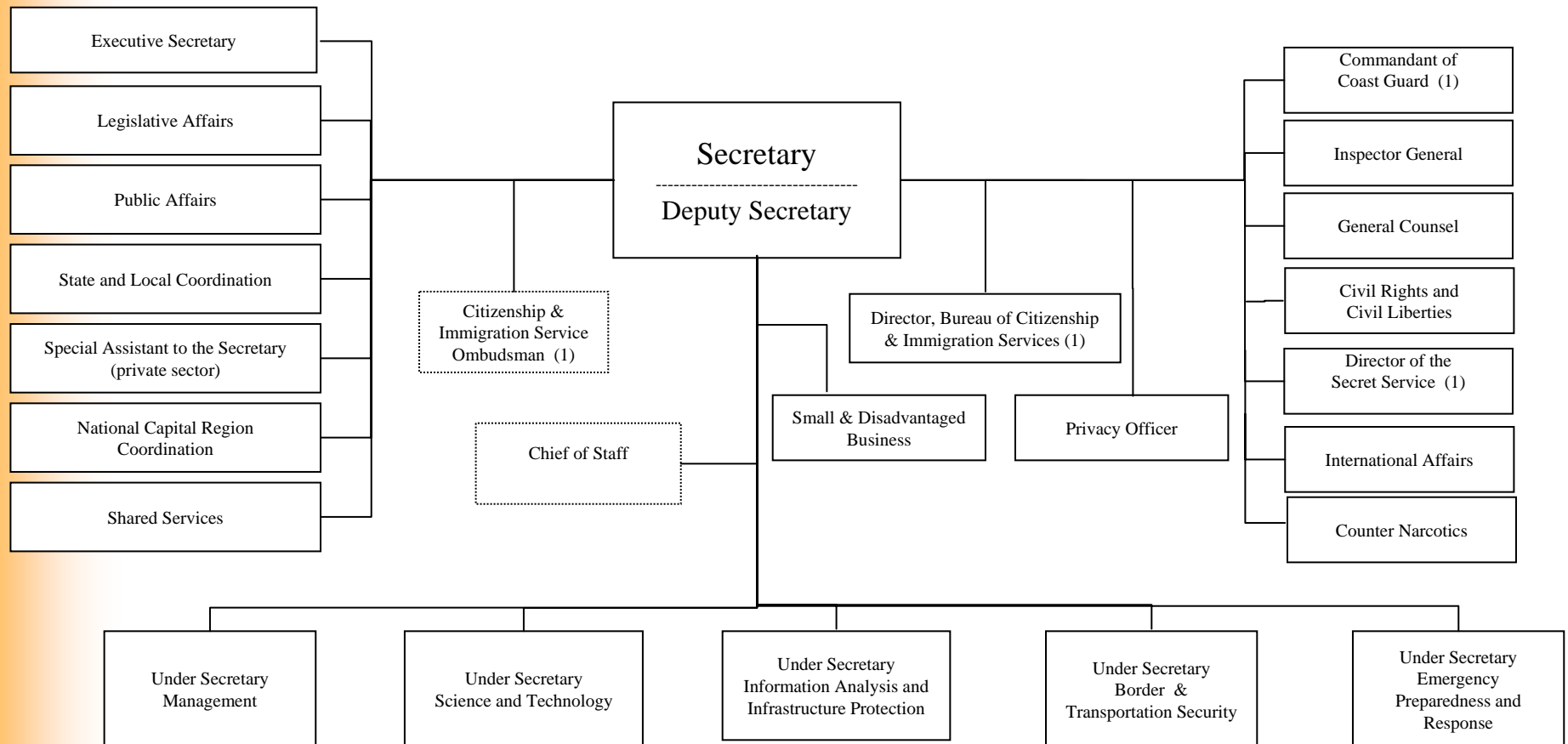


The DHS Umbrella

- **Border and Transportation Security**
 - The U.S. Customs Service (Treasury)
 - The Immigration and Naturalization Service (part) (Justice)
 - The Federal Protective Service
 - The Transportation Security Administration (Transportation)
 - Federal Law Enforcement Training Center (Treasury)
 - Animal and Plant Health Inspection Service (part)(Agriculture)
 - Office for Domestic Preparedness (Justice)
- **Emergency Preparedness and Response**
 - The Federal Emergency Management Agency (FEMA)
 - Strategic National Stockpile and the National Disaster Medical System (HHS)
 - Nuclear Incident Response Team (Energy)
 - Domestic Emergency Support Teams (Justice)
 - National Domestic Preparedness Office (FBI)
- **Science and Technology**
 - CBRN Countermeasures Programs (Energy)
 - Environmental Measurements Laboratory (Energy)
 - National BW Defense Analysis Center (Defense)
 - Plum Island Animal Disease Center (Agriculture)
- **Information Analysis and Information Protection**
 - Critical Infrastructure Assurance Office (Commerce)
 - Federal Computer Incident Response Center (GSA)
 - National Communications System (Defense)
 - National Infrastructure Protection Center (FBI)
 - Energy Security and Assurance Program (Energy)
- **US Secret Service**
- **US Coast Guard**

The DHS Org Structure

Department of Homeland Security





Current Regulations

To name a few of the current heavy-hitters...

- GLBA – Financial Institutions Security
- HIPAA – Health Care Security
- NERC 1200 UAS (FERC SMD) – Electric Grid Security
- CJIS – Justice Information Systems Security
- Sarbanes-Oxley (SOXA) – Financial Security (public)

Not to mention the others...

- SPS – Port Security
- California and Florida State Law precedents...
- 6 CFR 29 – DHS: Critical Infrastructure Information
- 33 CFR 101-106 – USCG: Maritime Security
- 49 CFR 172 – DOT: Hazmat Transportation



The Secret...

The secret to perpetual regulatory compliance?

Good security to start!

Don't wait for regulations to begin securing your organization, or you will always be behind

As usual, there is no "silver bullet" and the real solution is to actually do the hard work...



Get Involved

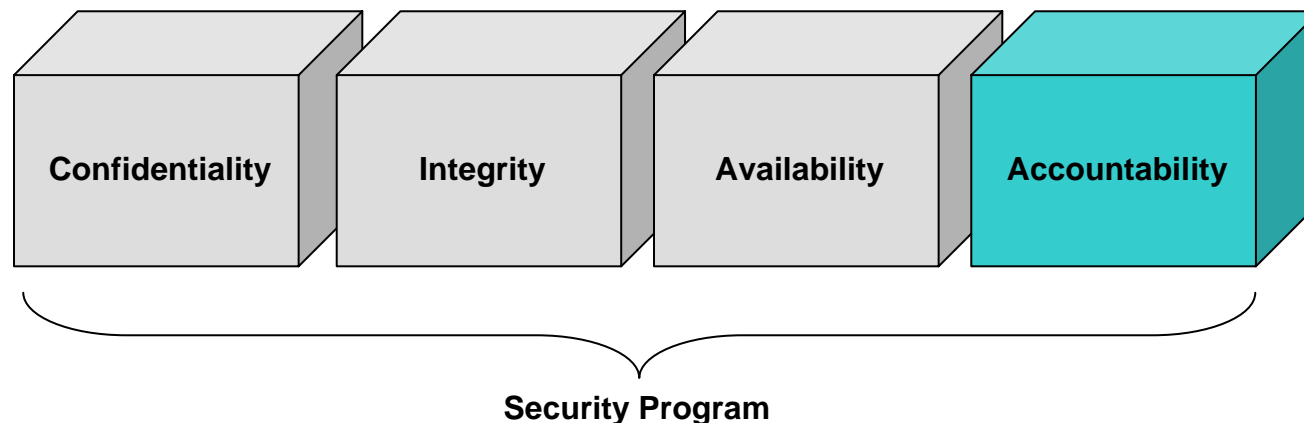
The real key is to be proactive...

- Minimize the “Ostrich Factor” - awareness
- Minimize the “Not Me Factor” - accountability
- Industry regulatory working groups
- Conferences and seminars
- Direct contact with regulatory agencies
- Provide a dedicated resource to drive compliance efforts
- Internal discussion within organization
- Get Executive awareness and support

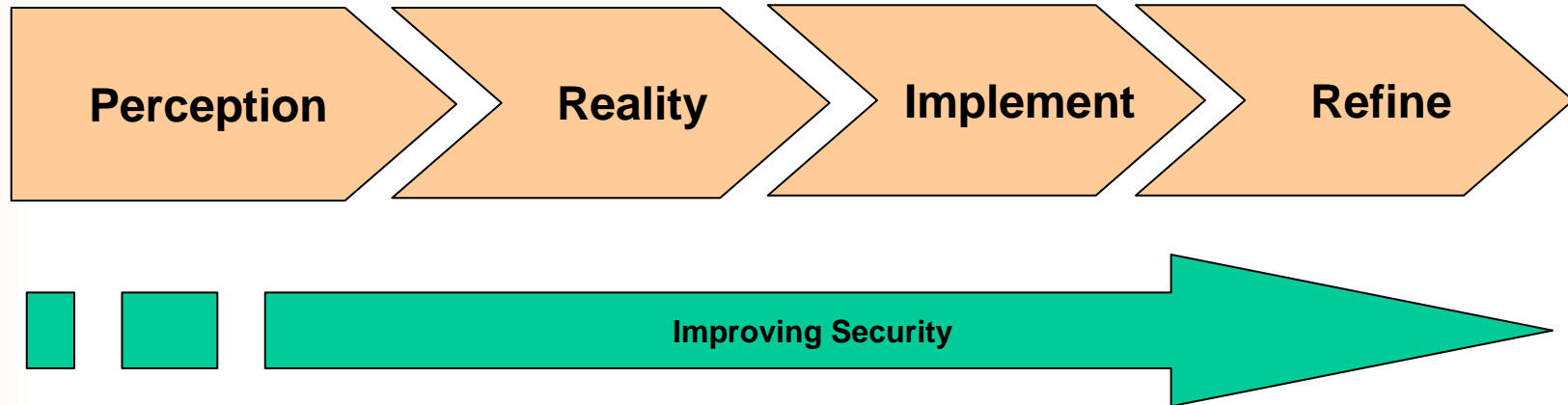
How can Security help?

- The environment is bad, very bad – but there are ways to succeed, safely and securely
- Many of the regulations and best practices strongly recommend the establishment/use of a dedicated security function for the organization
- What do you get with a dedicated security function?

The Goal:



Security Program Concepts



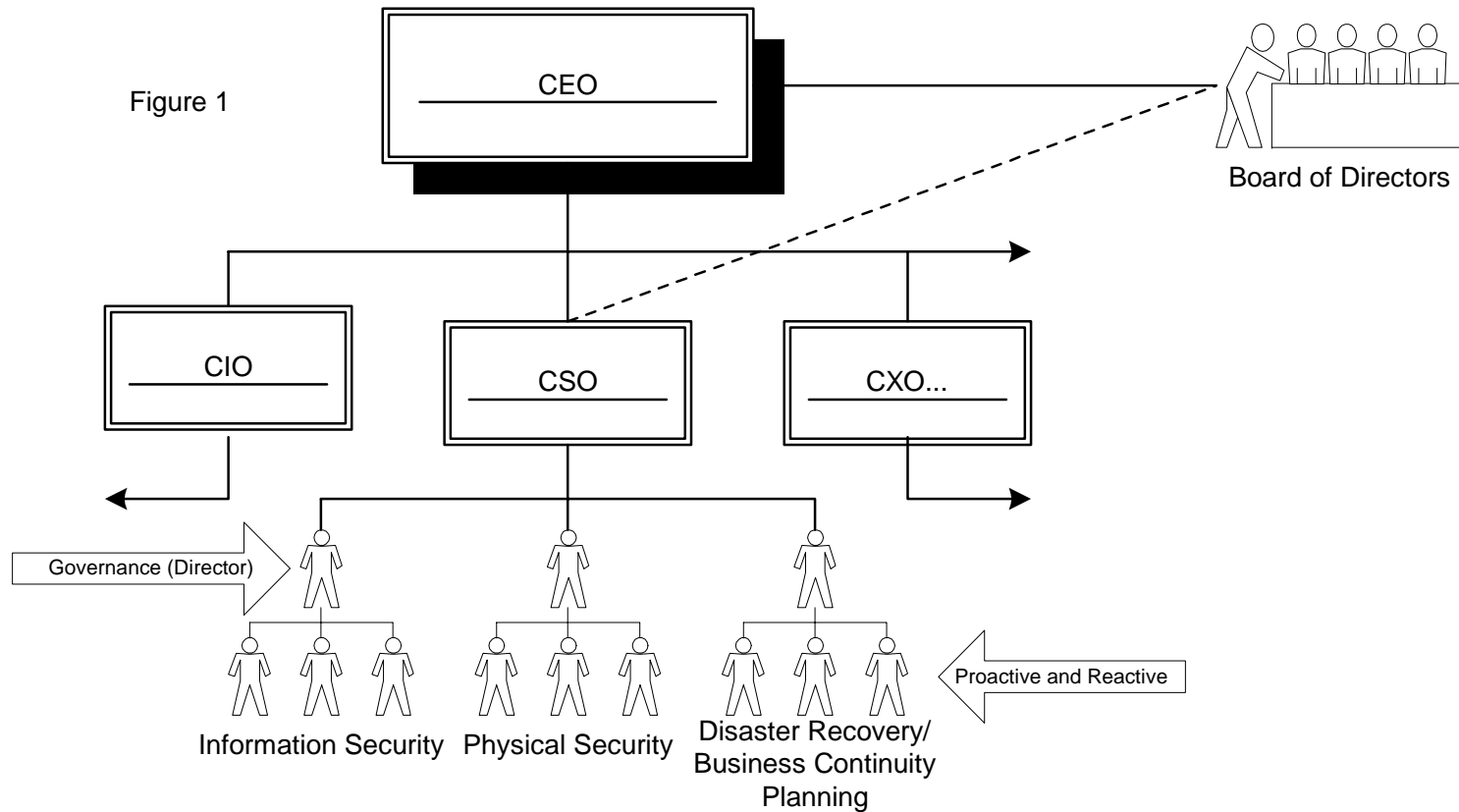
- **Perception = Is security important?**
- **Reality = How bad is it?**
- **Implement = What to do and when?**
- **Refine = How to improve?**



Security Program Components

- Security Management (Governance)
 - Authorization
 - Inter-organizational Communication
 - Policy
- Security Planning (Proactive)
 - Long-term Goals
 - Security Architecture
- Security Operations (Reactive)
 - Monitoring
 - Response

Best Practice Security Organization



Not the only option out there...



Security Program Priorities

- Risk (Assessment)
 - Determine just how bad it really is...
 - Start with biggest risks first
- Budget & Resources
 - Obtain the necessary resources to do the job
 - *May be the hardest task of all...*
- Compliance (Gap Analysis)
 - Where are you and where do you need to be relative to current and future regulations?
- Metrics and Benchmarking
 - Provide assurance that:
 - Security is being performed adequately
 - You are not only compliant to regulations today, but always



Security Program Metrics

- Better than the mythical “ROSI”
- Measure your Security over time
 - Patch/vulnerability management
 - Malicious code (virus, worm, etc) management
 - SPAM and inappropriate content management
 - Intrusion Detection (IDS) and Integrity Assurance alerts
 - Assessments, both self and external
 - Capability/Maturity; *ISO/IEC 21827*



Frameworks for Compliance

**So you are assessing and measuring
everything, now what?**

**Adopt a proven framework that is
repeatable and provides long-term
compliance assurance. A good
starting point is ISO 21827...**

CMM (ISO 21827) Framework

Process Areas:

- Groups of Base Practices
- Defined set of processes
- Collective in nature

Capability Levels:

- Phases of maturity
- Range of expected results
- Process oriented

	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Process Area 1	X	X	X			
Process Area 2	X	X	X	X		
Process Area 3	X	X	X			



The CMM Matrix

The Basic Model, applied...

Capability Levels...

Process Areas...

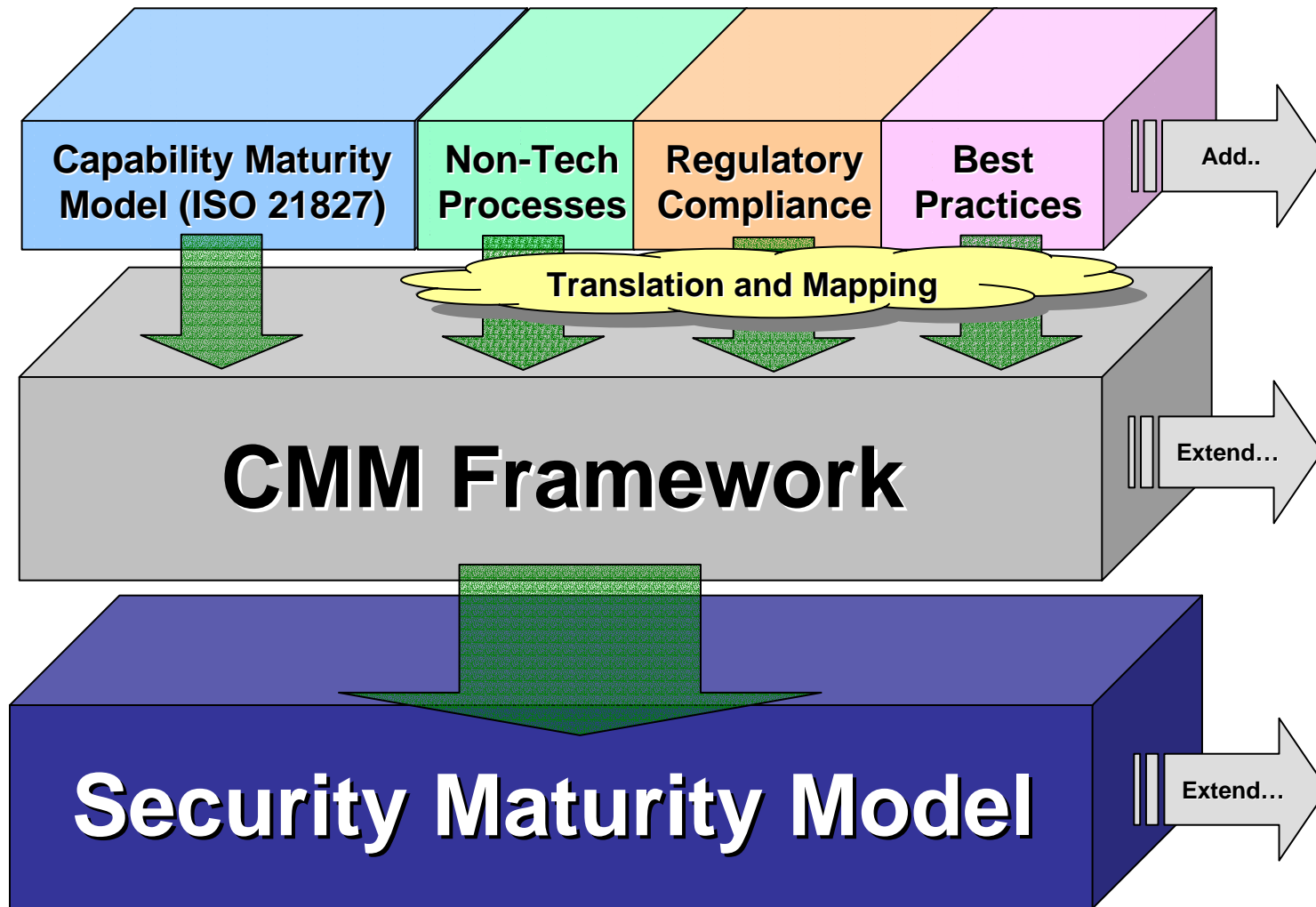
	Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Well Defined – 3	Quantitatively Controlled – 4	Continuously Improving – 5
Administer Security Controls	X	X	X			
Assess Impact	X	X				
Assess Security Risk	X	X	X			
Assess Threat	X	X				
Assess Vulnerability	X	X	X			
Build Assurance Argument	X	X				
Coordinate Security...	X	X	X			



Flexibility in the Model

- **Process Areas are not finite**
 - Add organization-specific Base Practices
 - Add Regulatory Requirements
 - Add Industry Initiatives
 - Add Security Best Practices
- **Capability Levels are not finite**
 - Can be expanded to be more granular
- **Fully Customizable...**
- **CMM Framework is the core...**

Security Maturity Model Stack



Sample HIPAA CMM Summary

HIPAA Compliance Bar

"Reasonable and Appropriate"

High-Level HIPAA Administrative Security Maturity Summary

Capability Levels

Security Process Areas

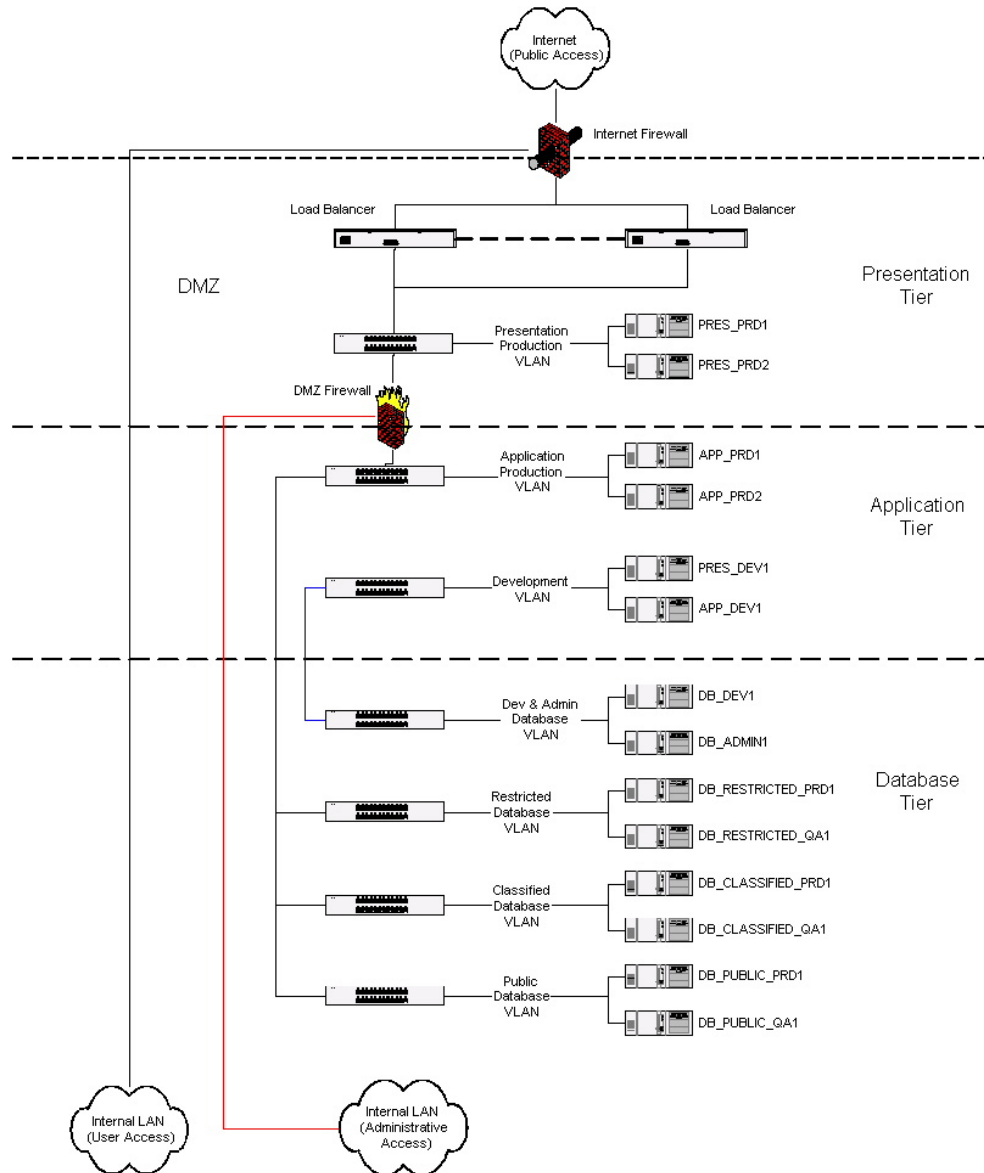
	Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Well Defined – 3	Quantitatively Controlled – 4	Continuously Improving – 5
Security Management	X	X	X			
Human Resource Management	X	X	X	X		
Security Awareness Training	X	X	X			
Operational Security	X	X	X	X		
Security Incident Procedures	X	X	X			
Contingency Planning	X	X	X	X		
Policy Review	X	X	X			
Administrative Security Maturity Score	2+					



e-Government Solutions

- e-Government is driving a lot of departments to allow public access to internal applications
 - In most cases the departments and their data are not classified, segmented or internally controlled
 - If one department is compromised it is an easy transition to the entire infrastructure
- In order to reduce the threat, create an n-tiered public portal
 - Common to all big ecommerce environments
 - Migrate all "e-Apps" into the public portal
 - Be sure to use appropriate controls between the public portal and the internal network.
- Access controls and other appropriate security controls should be included in the public portal as well

General *n*-Tier Architecture



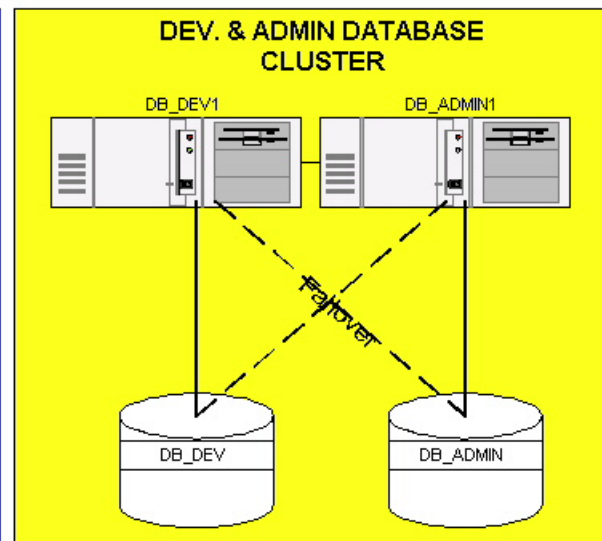
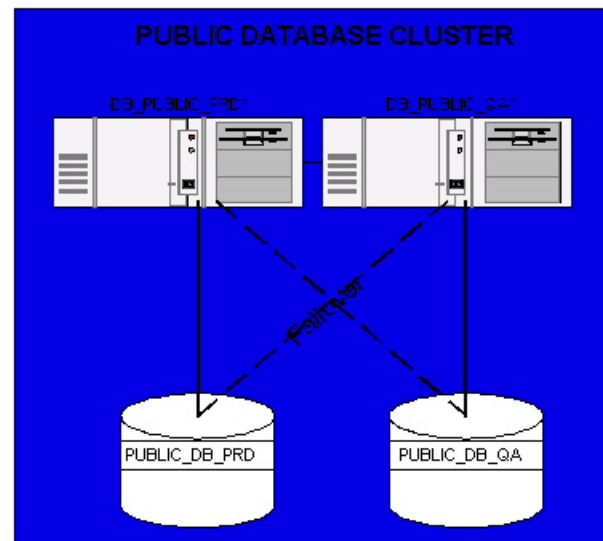
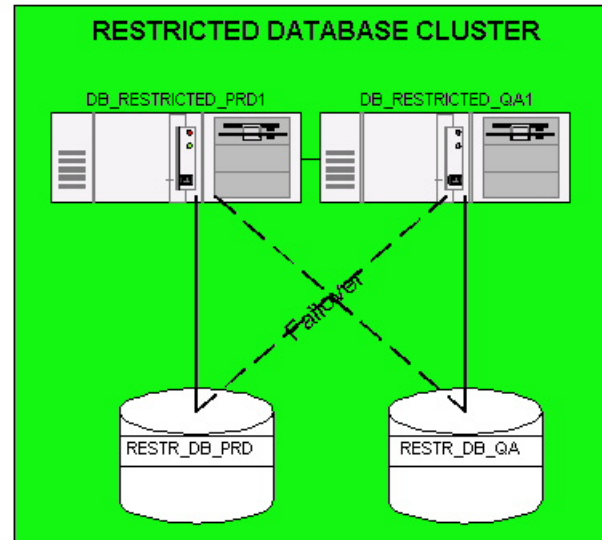
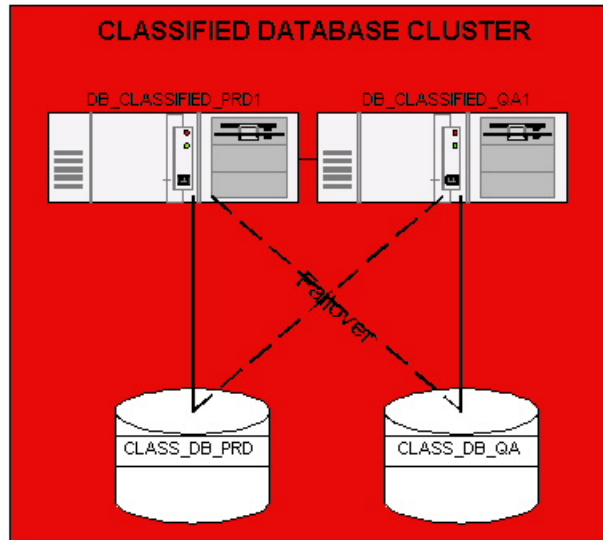
The *n* Tier Architecture is made up of the following layers:

- External Public Interface
 - Presentation Tier
 - Application Tier
 - Database Tier
- Support/Admin Tier

Insert additional layers if appropriate/necessary...

Establish Zones of Trust (1-100) for each layer...

Clustered Database Model





E-Gov Security Basics

- Layered Security
 - Defense in depth
 - Based on Classification and “Least Privileged” Model
 - The most sensitive data is behind several layers
 - Segment data using security zones with defined trust levels
- Access & Audit Controls
 - “Deny all policy” vs. “Accept all”
 - Authorization comes from system & data owners only
 - An formal authorization process must exist and based on a “need to know” model.
 - Audit controls must be automated.
 - Audit controls should exist between all security zones
 - The longer an event goes unnoticed the more impact it will have

Measure your success and provide visibility into processes



The Overall Plan...

- Pay attention to the agencies and industry working groups for new regulations; get involved in the development of standards
- Get visibility, support and awareness of Executives and Upper Management
- Obtain the funding and resources to implement necessary security controls by presenting real data and measuring success
- Establish a compliance framework that supercedes most current regulations, such as ISO 17799 or 21827, but doesn't go too far beyond what is appropriate
- Ensure the e-Government solution is secure through regular assessment and metrics



Useful Links...

Health Insurance Portability and Accountability Act (HIPAA)

- <http://aspe.hhs.gov/admsimp/faqtx.htm>
- <http://aspe.hhs.gov/admsimp/index.shtml>
- <http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm>
- http://www.hipaadvisory.com/action/faqs/faq_main.htm

The Department of Homeland Security

- <http://www.nipcr.gov/dailyreports/dailyindex.htm> - DHS IAIP Daily Report
- <http://www.dhs.gov/dhspublic/display?theme=10> - Grants from the DHS
- <http://www.dhs.gov/dhspublic/display?theme=13&content=3345> – DHS Org

NIST

- <http://csrc.nist.gov/publications/nistpubs/> - 800 Series
- <http://icat.nist.gov/icat.cfm> - ICAT CVE Search Engine (Metabase)

General e-Government Links

- <http://www.whitehouse.gov/omb/egov/>
- http://europa.eu.int/information_society/programmes/egov_rd/text_en.htm
- <http://www.centre-for-egovernment.com>
- <http://www.egovos.org/>



Questions?

Patrick C Miller, CISSP SSCP IAM
Principal Energy Security Advisor;
energy@breakwatersecurity.com
1.877.952.5500