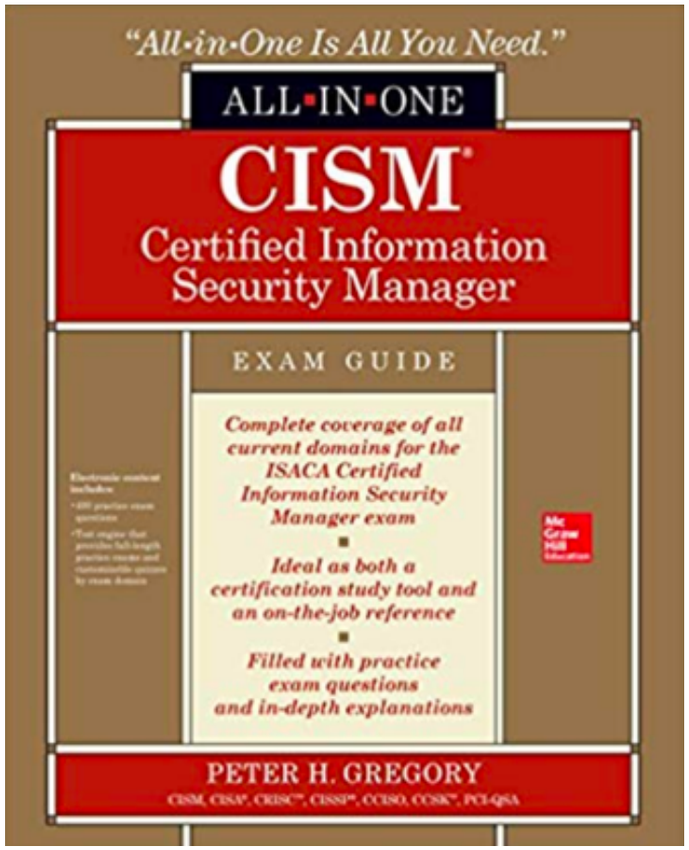
CNIT 160: Cybersecurity Responsibilities

2. Information Security Governance
Part 2

Pages 55 - 94

Updated 8-30-23



Topics in Part 1

- **Introduction to Information Security Governance**
- **Reason for Security Governance**
- **Security Governance Activities and Results**
- **Business Alignment**
- **Roles and Responsibilities**

Topics in Part 1 (continued)

- **Introduction to Information Security Governance (continued)**
  - **Monitoring Responsibilities**
  - **Information Security Governance Metrics**
  - **The Security Balanced Scorecard**
  - **Business Model for Information Security**

Topics in Part 2

- **Security Strategy Development**
  - **Strategy Objectives**
  - **Control Frameworks**
  - **Risk Objectives**
  - **Strategy Resources**
  - **Strategy Development**
  - **Strategy Constraints**

Strategy

- **The plan to achieve an objective**

Strategy Objectives

Strategy Objectives

- **Strategic alignment** The desired future state, and the strategy to get there, must be in alignment with the organization and *its* strategy and objectives.
- **Effective risk management** A security program must include a risk management policy, processes, and procedures. Without risk management, decisions are made blindly without regard to their consequences or level of risk.
- **Value delivery** The desired future state of a security program should include a focus for continual improvement and increasing efficiency. No organization has unlimited funds for security; instead, organizations need to reduce risk for the lowest reasonable cost.

Strategy Objectives

- **Resource optimization** Similar to value delivery, strategic goals should efficiently utilize available resources. Among other things, this means having only the necessary staff and tools to meet strategic objectives.
- **Performance measurement** While it is important for strategic objectives to be SMART, the ongoing security and security-related business operations should themselves be measurable, giving management an opportunity to drive continual improvement.
- **Assurance process integration** Organizations typically operate one or more separate assurance processes in silos that are not integrated. An effective strategy would work to break down these silos and consolidate assurance processes, reducing hidden risks.

Control Frameworks

Control Frameworks

- **COBIT**
- **ISO/IEC 27001**
- **ISO/IEC 38500**
- **ITIL / ISO/IEC 20000**
- **HIPAA**
- **NIST SP 800-53**
- **NIST CSF**
- **CIS 20**
- **PCI-DSS**

COBIT

- **Control Objectives for Information and Related Technologies**
- **Developed by IT Governance Institute and ISACA**
- **Four domains**
  - **Plan and Organize**
  - **Acquire and Implement**
  - **Deliver and Support**
  - **Monitor and Evaluate**

COBIT

- **An IT process framework**
- **Not primarily a security framework**
- **37 processes, including these security- and risk-related ones**
  - **Ensure risk optimization**
  - **Manage risk**
  - **Manage security**
  - **Manage security resources**
  - **Monitor, evaluate, and assess compliance with external requirements**

ISO/IEC 27001

- **International standard for information security and risk management**
- **Two sections: Requirements and Controls**
- **Highly respected**
- **Costs $117 for standards documents**
- **Costs thousands and takes up to 12 months to achieve**

ISO/IEC 27001 Requirements

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

ISO/IEC 27001 Controls

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security

ISO/IEC 27001 Controls

- **Operations security**
- **Communications security**
- **System acquisition, development, and maintenance**
- **Supplier relationships**
- **Information security incident management**
- **Information security aspects of business continuity management**
- **Compliance**

ISO/IEC 38500

- **Governance of IT for the Organization**
- **International standard for corporate governance of information technology**

ITIL / ISO/IED 20000

- **IT Infrastructure Library (ITIL)**
- **Framework of processes for IT service delivery and IT service management**
- **Developed by the UK**

HIPAA

- **Health Insurance Portability and Accountability Act**
- **Protection of Electronic Protected Health Information (EPHI)**
- **Requirements for**
  - **Administrative safeguards**
  - **Physical safeguards**
  - **Technical safeguards**

NIST SP 800-53

- **From US National Institute for Standards and Technology**
- **NIST Special Publication (SP) 800-53**
- **"Security and Privacy Controls for Federal Information Systems and Organizations"**
- **Well-known, widely adopted**
- **Required for all US gov't systems**
- **And others handling gov't information**

NIST SP 800-53
18 Categories

- **Access control**
- **Awareness and training**
- **Audit and accountability**
- **Security assessment and authorization**
- **Configuration management**
- **Contingency planning**
- **Identification and authentication**
- **Incident response**
- **Maintenance**

NIST SP 800-53
18 Categories

- **Media protection**
- **Physical and environmental protection**
- **Planning**
- **Personnel security**
- **Risk assessment**
- **System and services acquisition**
- **System and communications protection**
- **System and information integrity**
- **Program management**

NIST Cybersecurity Framework (NIST-CSF)

- **Risk-based lifecycle methodology for**
  - **Assessing risk**
  - **Enacting controls**
  - **Measuring control effectiveness**
- **Similar to ISO/IEC 27001**

NIST-CSF Components

- **Framework Core** These are a set of functions—Identify, Protect, Detect, Respond, Recover—that make up the life cycle of high-level functions in an information security program. The Framework Core includes a complete set of controls (known as *references*) within the four activities.
- **Framework Implementation Tiers** These are maturity levels, from least mature to most mature: Partial, Risk Informed, Repeatable, Adaptive.
- **Framework Profile** This is an alignment of elements of the Framework Core (the functions, categories, subcategories, and references) with an organization's business requirements, risk tolerance, and available resources.

Center for Internet Security Critical Security Controls

- **CSC framework from the Center for Internet Security (CIS)**
- **From SANS 20 Critical Security Controls**

SANS 20 Critical Security Controls

- **Inventory of Authorized and Unauthorized Devices**
- **Inventory of Authorized and Unauthorized Software**
- **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
- **Continuous Vulnerability Assessment and Remediation**
- **Controlled Use of Administrative Privileges**
- **Maintenance, Monitoring, and Analysis of Audit Logs**
- **E-mail and Web Browser Protections**
- **Malware Defenses**
- **Limitation and Control of Network Ports, Protocols, and Services**
- **Data Recovery Capability**

SANS 20 Critical Security Controls

- **Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
- **Boundary Defense**
- **Data Protection**
- **Controlled Access Based on the Need to Know**
- **Wireless Access Control**
- **Account Monitoring and Control**
- **Security Skills Assessment and Appropriate Training to Fill Gaps**
- **Application Software Security**
- **Incident Response and Management**
- **Penetration Tests and Red Team Exercises**

PCI-DSS

- **Payment Card Industry Data Security Standard**
- **From the PCI Standards Council**
  - **Consortium of credit card brands**
    - **Visa, MasterCard, AmEx, Discover, and JCB**

PCI-DSS
12 Control Objectives

- **Install and maintain a firewall configuration to protect cardholder data.**
- **Do not use vendor-supplied defaults for system passwords and other security parameters.**
- **Protect stored cardholder data.**
- **Encrypt transmission of cardholder data across open, public networks.**
- **Protect all systems against malware and regularly update antivirus software or programs.**
- **Develop and maintain secure systems and applications.**

PCI-DSS
12 Control Objectives

- **Restrict access to cardholder data by business need to know.**
- **Identify and authenticate access to system components.**
- **Restrict physical access to cardholder data.**
- **Track and monitor all access to network resources and cardholder data.**
- **Regularly test security systems and processes.**
- **Maintain a policy that addresses information security for all personnel.**

Ch 2b-1

Risk Objectives

Risk Objectives

- **Difficult to quantify risk**
- **Often just rated as "high/medium/low"**
- **Little more than guesswork**

Strategy Resources

Two Types of Inputs

- **Risk assessments**
- **Threat assessments**

Other Inputs

- Policy
- Standards
- Guidelines
- Processes and procedures
- Architecture
- Controls
- Skills
- Metrics
- Assets
- Risk ledger
- Insurance
- Critical data
- Business impact analysis
- Security incident log
- Outsourced services
- Audits
- Culture
- Maturity
- Risk appetite

Risk Assessment

- **Should drive creation of strategic objectives**
- **Sometimes done merely for compliance**

Threat Assessment

- **Focuses on external threats**
- **Vulnerabilities change frequently**
- **Threats are more constant**

Policy

- **Aspects**
  - **Breadth of coverage**
  - **Relevance**
  - **Strictness**
  - **Accountability and consequences**
  - **Compliance**
  - **Periodic management review**

Standards

- **Detailed methods, specifications, brands, and configurations to use throughout the organization**
- **Similar concerns as policy, but also**
  - **How were standards developed?**
    - **Often from NIST or such groups**
  - **How good are they?**

Guidelines

- **Many organizations don't get further than creating policies and standards**
- **Proper guidelines indicate maturity**
- **Guidance how to adhere to policy**

Processes and Procedures

- **Documents indicate maturity**
- **Interviews of personnel required to assess effectiveness**
- **And whether processes are carried out as designed**

Architecture

- **Layout of infrastructure**
- ***Technical debt***
  - **Poor design**
  - **Outdated and unsupported components**

Controls

- **Controls may be only on paper, not practice**
- **Examine:**
  - **Control owners**
  - **Purpose and scope**
- **May be part of a control framework**
  - **ISO 27001, NIST 800-53, HIPAA, PCI**

Skills

- **Tenure This includes how many years of different types of experience a staff member may have.**
- **Behavioral This includes leadership, management, coordination, and logistics.**
- **Disciplines This includes fields such as systems engineering, network engineering, controls development, audit, risk management, and risk analysis.**
- **Technologies This includes skills with specific technologies such as Palo Alto Networks firewalls, CentOS operating systems, Logrhythm, and AppScan.**

Metrics

- **Guide long-term effectiveness of controls**
- **Consider target audience**
- **See if metrics were delivered**
- **If they were used to make tactical or strategic changes**

Assets

- **Vulnerability management**
  - **Identify the environment to be scanned.**
  - **Scan assets for vulnerabilities.**
  - **Identify and categorize vulnerabilities.**
  - **Remediate vulnerabilities (often through applying security patches but sometimes through configuration changes or increased monitoring and alerting).**

Risk Ledger

- **History and findings from risk assessments, threat assessments, vulnerability assessments, incidents, etc.**
- **Lack of a risk ledger indicates**
  - **Compliance-based security, or**
  - **Asset-based or ad hoc**
  - **Both low maturity states**

Vulnerability Assessment

- **Indicates**
  - **Operational maturity**
  - **Security maturity**

Insurance

- **Why was insurance purchased?**
  - **Compliance**
  - **Customer requirement**
  - **Prior incidents**
  - **Risk treatment**

Critical Data

- **Most organizations don't know well where their data is or how it's used**
- **Especially on cloud services**
- **BYOD (Bring Your Own Device)**

Business Impact Analysis

- **Determining Maximum Tolerable Downtime**
  - **For processes and resources**
- **Cornerstone of Business Continuity and Disaster Recovery planning**
- **Presence of BIA indicates good maturity**

Security Incident Log

- **May be sparse in immature, compliance-based organizations**
- **Mature organizations will have post-mortem analysis and direct changes**
- **Lack of/deficient SIEM**
- **Training personnel to recognize a security incident**

Outsourced Services

- **Most business apps moving to the cloud**
  - **IaaS, PaaS, Saas**
- **Most important: amount of due care**
- ***Third-party risk***
  - **Up-front due diligence**
  - **Relationship risk assessment**
  - **Ongoing due diligence**

Audits

- **Internal and external**
- **Audit features:**
  - **Objective**
  - **Scope**
  - **Qualifications of auditors**
  - **Audit methodologies**

Culture

- **People are absolutely key**
- **Technology cannot compensate for bad culture**
- **Aspects:**
  - **Leadership**
  - **Accountability**
  - **Empowerment**
  - **Security awareness**

Maturity

- **Overall measure**
- **Varies for different aspects of security program**

Ch 2b-2

Strategy Development

Strategic Objectives

- **Improvements in protective controls**
- **Improvements in incident visibility**
- **Improvements in incident response**
- **Reductions in risk, including compliance risk**
- **Reductions in cost**
- **Increased resiliency of key business systems**

Examples

Examples of broad, sweeping objectives for developing new security capabilities include the following:

- **Define and implement a SIEM to provide visibility into security and operational events.**
- **Define and implement a security incident response program.**
- **Define and implement a security awareness learning program.**

Examples

Examples of objectives for improving existing capabilities include the following:

- **Integrate vulnerability management and GRC systems.**
- **Link security awareness and access management programs so that staff members must successfully complete security awareness training to retain their system access.**

Gap Assessment

- **Difference between current and desired state**
- **Must understand starting point**
  - **Existing/previous strategy**
  - **Security charter, policy, standards, procedures, guidelines, controls**
  - **Risk assessments**
  - **Internal and external audit results**
  - **Security metrics**
  - **Risk ledger**

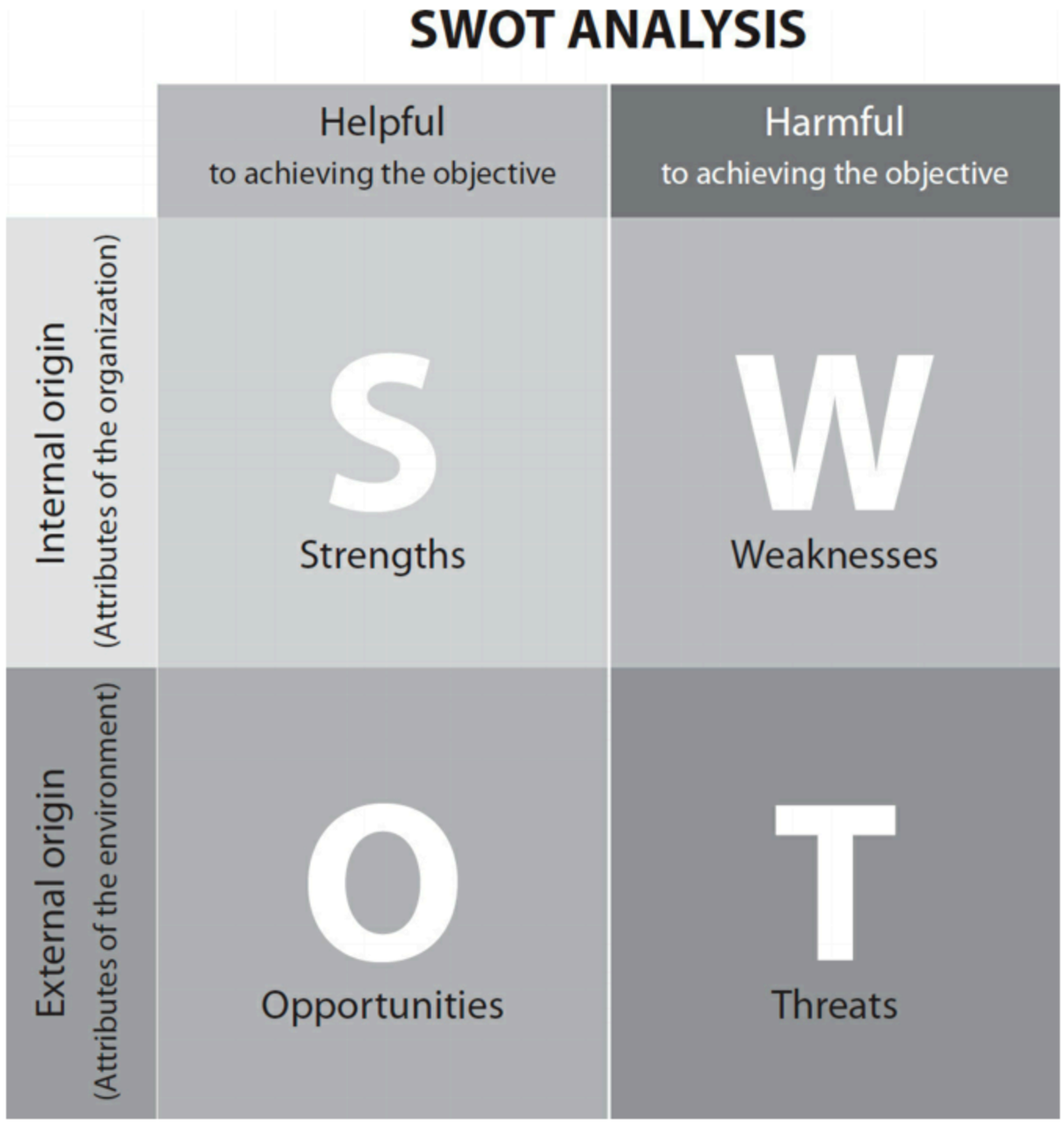
Gap Assessment

- **Must understand starting point (continued)**
  - **Risk treatment decision records**
  - **Security incident program and records**
  - **Third-party risk**
  - **Business continuity and disaster recovery program**
  - **Security awareness training program**
  - **IT and security projects**

Examining a Security Program

- **Absence of evidence is not evidence of absence**
- **Freshness, usefulness, and window dressing**
- **Scope, turf, and politics**
- **Reading between the lines**
- **Off the books**
- **Regulatory requirements**

Strengths, Weaknesses, Opportunities, Threats Analysis (SWOT)



Capability Maturity Models

- **CMMi-DEV**
- **Capability Maturity Model Integration for Development**
- **From Carnegie-Mellon University**

CMMi-DEV
Levels of Maturity

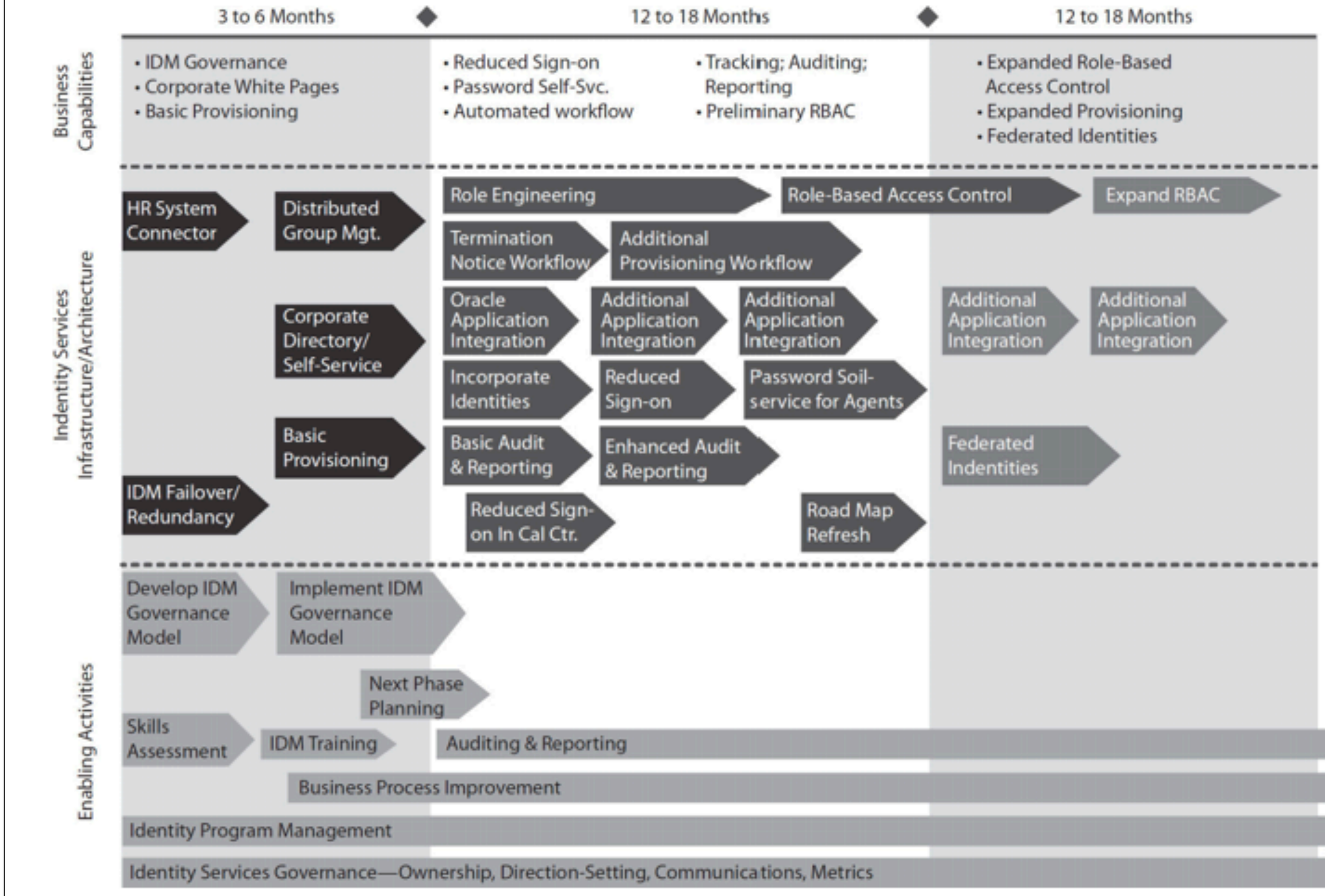
- **Level 1: Initial** This represents a process that is ad hoc, inconsistent, unmeasured, and unrepeatable.
- **Level 2: Repeatable** This represents a process that is performed consistently and with the same outcome. It may or may not be well-documented.
- **Level 3: Defined** This represents a process that is well-defined and well-documented.
- **Level 4: Managed** This represents a quantitatively measured process with one or more metrics.
- **Level 5: Optimizing** This represents a measured process that is under continuous improvement.

Maturity Models

- **Level 5 is not the ultimate objective**
  - **For most organizations, levels 2.5 to 3.5 is good enough**
- **Each control or process may have its own maturity level**

Road Map Development

- **Steps required to achieve a strategic objective**
- **Next page shows an example for identity and access management**


3 to 6 Months
12 to 18 Months
12 to 18 Months
Business Capabilities
• IDM Governance
• Corporate White Pages
• Basic Provisioning
• Reduced Sign-on
• Password Self-Svc.
• Automated workflow
• Tracking; Auditing; Reporting
• Preliminary RBAC
• Expanded Role-Based Access Control
• Expanded Provisioning
• Federated Identities
Identity Services Infrastructure/Architecture
HR System Connector
Distributed Group Mgt.
Role Engineering
Role-Based Access Control
Expand RBAC
Termination Notice Workflow
Additional Provisioning Workflow
Corporate Directory/ Self-Service
Oracle Application Integration
Additional Application Integration
Additional Application Integration
Additional Application Integration
Additional Application Integration
Incorporate Identities
Reduced Sign-on
Password Soil-service for Agents
Basic Provisioning
Basic Audit & Reporting
Enhanced Audit & Reporting
Federated Indentities
IDM Failover/ Redundancy
Reduced Sign-on In Cal Ctr.
Road Map Refresh
Enabling Activities
Develop IDM Governance Model
Implement IDM Governance Model
Next Phase Planning
Skills Assessment
IDM Training
Auditing & Reporting
Business Process Improvement
Identity Program Management
Identity Services Governance—Ownership, Direction-Setting, Communications, Metrics

Policy Development

- **"Rules of the road" for employees**
- **Commonly based on frameworks**
  - **NIST SP 800-53**
  - **ISO 27001**
  - **HIPAA/HITECH**
  - **PCI-DSS**
  - **CIS CSC 20**

Controls Development

- **Changes to control narrative**
  - **Which describe controls in detail**
- **Changes to scope**
- **Changes in control testing**
- **Entirely new control**

Selecting a Control Framework

- **Typically a choice between**
  - **CIS CSC**
  - **ISO/IEC 27002**
  - **NIST 800-53**
- **They are all similar**

Standards Development

- **Policies define *what* is to be done**
- **Standards define *how* policies are carried out**
- **Policies are unspecific but long-lasting**
- **Standards are specific but change more frequently**

Standards Development

Standards need to be developed carefully, for several reasons:

- **They must properly reflect the intent of one or more corresponding policies.**
- **They will have to be able to be successfully implemented.**
- **They need to be unambiguous.**
- **Their directives will need to be able to be automated, where large numbers of systems, endpoints, devices, or people are involved, leading to consistency and uniformity.**

Examples of Standards

- **Protocol**
- **Vendor**
- **Configuration**
- **Programming language**
- **Methodology**
  - **Such as FAIR risk analysis, OCTAVE security assessments, and SMART for objectives**
- **Control frameworks**
  - **Such as NIST SP 800-53, PCI-DSS, HIPAA, COBIT, and ISO 27002**

Processes and Procedures

- **Identify undocumented processes and procedures and document them**
- **Develop procedures and standards so there is consistency among processes, procedures, and documents**
- **Consistent development and review**

Roles and Responsibilities

- **Job descriptions**
- **Department charter documents**
- **Department policy documents**
- **Roles and responsibility sections of process documents**

Training and Awareness

- **Important defense against phishing**
  - **General security awareness**
  - **New and updated processes and procedures**
  - **New and updated technologies**

Developing a Business Case

- **Problem statement**
- **Current state and desired state**
- **Success criteria**
- **Requirements**
- **Approach and Plan**

Business Case Characteristics

- **Alignment with organization**
- **Statements in business terms**

Establishing Communications and Reporting

- **Board of directors meetings**
- **Governance and steering committee meetings**
- **Security awareness**
- **Security advisories**
- **Security incidents**
- **Metrics**

Obtaining Management Commitment

- **Executives are often unaware of potency of modern threats**
  - **Mistakenly believe they are an unlikely target**
- **Security strategist must inform management**
  - **Without using FUD (Fear, Uncertainty, and Doubt)**

Normalcy Bias

- **Since no breach has occurred, things must be OK**

Strategy Constraints

Strategy Constraints

- **Basic Resistance to Change**
- **Culture**
  - **Strong or healthy**
  - **Weak**
  - **Culture of fear**

Strategy Constraints

- **Organizational Structure**
- **Staff Capabilities**
- **Budget and Cost**
- **Time**
- **Legal and Regulatory Obligations**
- **Acceptable Risk**

Organizational Inertia

- **Operational people performing changes**
  - **Must work slowly and carefully to maintain operational and quality levels**
- **Learning curve**
- **Human resistance to change**

Ch 2b-3