

# Safeguarding the Enterprise



## Security Tools and Techniques

A White Paper by:

Thomas Bronack

[bronackt@gmail.com](mailto:bronackt@gmail.com)

# Safeguarding the Enterprise

## Security Tools and Techniques

### Contents

History.....	5
How Security Evolved: .....	5
Personnel Identification Systems.....	6
Protecting the Enterprise through a Continuous Diagnostic and Mitigation (CDM) System.....	7
The three phases of CDM Implementation .....	7
Phase 1: Endpoint Integrity and Resource Vulnerability Management.....	7
Phase 2: Least Privilege and Infrastructure Integrity.....	7
Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle .....	7
Phase Goals and Deliverables .....	7
CDM Three Phase approach project flow .....	8
Application Development and Data Sensitivity .....	9
Network Access.....	10
Recovery Operations using Domains. ....	11
Logon to a Domain with today's security protection.....	12
The Logon Process .....	12
Building and Protecting the Environment.....	13
What is required to protect our enterprise and society?.....	13
What are we protecting? .....	14
SIEM – Security Incident Event Management.....	14
SA - Security Analytics.....	15
SOC - Security Operations Center .....	15
Key Characteristics of SIEM and SA Platforms .....	16
Role Based Access Controls (RBAC) and Entitlements.....	16
Continuous Diagnostic and Mitigation (CDM) System.....	17
Continuous Diagnostic and Mitigation (CDM) project overview.....	17
How should an enterprise implement their security management system? .....	18
Automated Load Balancing and Error Handling.....	19
Organizational Considerations.....	21

---

Chief Information Security Officer (CISO) .....	21
Defining the needs and responsibilities of an Enterprise Security System .....	22
Defining Security and Technology threats and assigning Responsibilities .....	22
Information Security Responsibilities .....	22
Approaches to developing an Enterprise Security System .....	23
Threat based approach to implementing Enterprise Security Management .....	23
Risk based approach to Enterprise Security Management .....	24
Cloud Risk and Security Protection .....	24
Ten Recommended Network Security Tools.....	25
Appendix 'A' .....	29
COSO – Committee of Sponsoring Organizations (Risk Management Guidelines) .....	29
CobIT – Control Objectives for Information Technology (Converting Business to IT) .....	30
ITIL – Information Technology Infrastructure Library (Service Delivery and Support) .....	31
CMMI – Capability Maturity Model Integration (Optimizing Performance) .....	32
GRC – Governance, Regulations, and Compliance (Adhering to Laws and Regulations) .....	33
Supply Chain Management (Managing Supplies and their Delivery Locations) .....	34
Systems Management and Controls – Workflow .....	35
Systems Management Organizational Structure .....	36
SDLC – Systems Development Life Cycle (Migrating Applications to Production) .....	37

## Table of Figures:

Figure 1: Tom Bronack, author of White Paper – bronackt@dcagl.com.....	5
Figure 2: Overview of the CDM Dashboard System's Three Phases.....	8
Figure 3: Internet Protocol (IP) Delivery System (Local / Remote).....	11
Figure 4: Logging on to a Domain with the latest security precautions. ....	12
Figure 5: The Logon Function of Applid, Userid, Password (with a Domain Passcode included).....	12
Figure 6: Domain workload segments and recovery operations.....	13
Figure 7: Protecting Enterprise Data from outside intrusion with layers of protection.....	14
Figure 8: Security Operations Center (SOC).....	15
Figure 9: Features of a SIEM and Security Analytics System .....	16
Figure 10: The Goals of a Continuous Diagnostic and Mitigation (CDM) Dashboard System .....	17
Figure 11: Load Balancing and Error Handling for a Virtual Environment with Automatic Recovery .....	19
Figure 12: The enterprise security and compliance organizational structure.....	21
Figure 13: Defining Security and Technology Threats and Assigning Responsibilities .....	22
Figure 14: Threat Based Approach to implementing an Enterprise Security System.....	23
Figure 15: Risk Based Approach to implementing an Enterprise Security System .....	24
Figure 16: COSO - Risk Assessment Best Practices .....	29
Figure 17: CobIT Framework - Control Objectives for Information Technology.....	30
Figure 18: ITIL v3 - Information Technology Infrastructure Library.....	31
Figure 19: CMMI - Capability Maturity Model Integration .....	32
Figure 20: GRC (Governance, Regulations, and Compliance) Adherence.....	33
Figure 21: Supply Chain Management.....	34
Figure 22: Systems Management Disciplines described.....	35
Figure 23: Systems Management Organizational Structure .....	36
Figure 24: Systems Development Life Cycle .....	37

## History

### How Security Evolved:

Ever since the 1960's, when a new era of Information technology (IT) began (remember IBM 360 Mainframes) there has always been a concern about safeguarding information from unauthorized intrusion and the loss of critical data.

At first, physical security (now referred to as a Physical Access System – PAS) stopped unauthorized people from entering the data center and gaining access to computers. For a long-time physical security proved sufficient, but then Information technology expanded to include Communications between the computer and the end-user, making physical security insufficient. It was necessary to create a new type of security system that would be used to control who had access to programs (referred to as Applications with a short hand name of Applid to identify them) and from which locations. The concept grew into a three-tiered Access Control System based on Applid, Userid, and Password, commonly referred to as your “**Log On.**”



Figure 1: Tom Bronack, author of White Paper – [bronackt@dcaqi.com](mailto:bronackt@dcaqi.com)

Again, this approach satisfied most requirements to safeguard information and locations, but times changed, and people got smarter in the use of computers. Eventually, Hackers started to get curious about what was in the mainframe and how they could play with it. That led to an entire revolution with “**Black Hats**” trying to gain unauthorized access and “**White Hats**” trying to block their attempts. Now, the entire computer field is like the “Wild-Wild-West” because of the World Wide Web (WWW) and the Internet.

Today, people can stay hidden behind walls and communicate over telephone lines and satellites to computers all over the world. These people are attempting criminal activities to steal a person's identity or access their bank account, with succeeding. Even worse, are State Sponsored Cyber Attacks aimed at stealing intellectual property, military secrets, or interfering with the infrastructure of countries.

These attacks could lead to a cyber-war that could end with everybody losing computer services, control over the infrastructure, and suffering a generational impact that would devastate society. We could all be living in the 19<sup>th</sup> century again and who wants that, who could even do the things people did then to survive? We have all grown up too accustomed to use computers and we may have lost our ability to survive without them.

Now you have an idea why information security is so important. The loss of computers would have a dramatic impact on society and drive people back to a time when they were not prepared to live in it again. How can we stop that from happening?

## Personnel Identification Systems

It has become imperative to **verify a person's identity** for security reasons, like voting or certifying that an individual has the authority to access physical and logical assets within an enterprise, whether that enterprise be governmental or corporate. These “**Access Rights**” certification systems include:

- **PAS** – Physical Access System (buildings, offices, etc.)
- **LAS** – Logical Access System (computer systems, files, applications, etc.)
- **CAC** – Common Access Card used by the Department of Defense
- **TWIC** – Transportation Worker Identification Card used by TSA and the Dept. of State

Access Rights are “**Entitlements**” based on the functional responsibilities performed by an individual as defined by their Job Title and stated in their job description. Having access to locations and assets is mandatory for completing assigned duties, so certifications allowing access to locations and assets are included in Entitlements. When a person changes job titles, they will assume the Entitlements of the new position and no longer have the Entitlements of their old position. Because of this, **Entitlements are assigned work positions, by title, and not an individual.**

Entitlements are access control **certificates** that define what assets (Physical / Logical) a person can access based on their job function. Access rights are CRUD (Create, Read, Update, and Delete) permissions and assigned to user groups or individuals. Security systems that provide compliance to these guidelines are referred to as “**Role Based Access Control (RBAC)**” systems (i.e., RSA Archer uses this approach for Security and Access Controls).

Most systems today use a **User id / Password** combination to allow entry to an application or service, but User id / Password Management is becoming difficult to control and often can be hacked. A better way to manage access is via a biometric smart card combined with end-to-end encryption / cryptography that is unique to an individual and does not require remembering a User id / Password. PINs prove a card is not stolen, or to deactivate a card.

Today, the US Government requires a **Personal Identification Verification** card (**PIV**) to control access to physical and logical assets and it replaces all the previous Access Systems listed above. The PIV Card can grant access to physical and logical assets, while generating audit trail records for tracking, analysis, and security processing. To track contractors within governmental organizations a **Personal Identification Verification - Interoperable** card (**PIV-I**) is used, which is like the PIV card. Together, these cards are **Unique Universal Identification** (UUID) Cards because they allow any enterprise to verify an individual's identity and allow access to a location, service, or product. Private Sector Enterprises can use the PIV-I Card to achieve the highest level of security and access control (i.e., Cryptographic, Bio-Metric, Encryption).

Another White Paper of mine reviews the history of personal identification verification and defines the laws and mandates adopted by the United States Government for adhering to Entitlements, through a RBAC security system using biometric PIV smart cards with end-to-end encryption and cryptography for optimum security precautions. The PIV card is for government use, while the PIV-I card is for private sector enterprises.

## Protecting the Enterprise through a Continuous Diagnostic and Mitigation (CDM) System

### The three phases of CDM Implementation

#### Phase 1: Endpoint Integrity and Resource Vulnerability Management

- HWAM – Hardware Asset Management
- SWAM – Software Asset Management
- CSM – Configuration Settings Management
- VUL – Vulnerability Management

#### Phase 2: Least Privilege and Infrastructure Integrity

- TRUST –Access Control Management (Trust in People Granted Access)
- BEHV – Security-Related Behavior Management
- CRED – Credentials and Authentication Management
- PRIV – Privileges
- Boundary Protection (Network, Physical, Virtual)

#### Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle

- Plan for Events
- Respond to Events (Real-Time Situational Awareness)
- Generic Audit/Monitoring (Traditional Audit Methods)
- Document Requirements, Policy, etc.
- Quality Management
- Risk Management

### Phase Goals and Deliverables

#### **Endpoint Integrity and Resource Vulnerability Management** – is:

- Validating the hardware and software management process,
- Establishing settings associated with product configurations, and
- Defining how Vulnerability Management is accomplished.

#### **Least Privilege and Infrastructure Integrity** – is responsible for

- Ensuring that personnel utilizing network facilities are provided with the access they are Entitled to,
- Conducting personnel background checks and defining their job functional responsibilities.
- Ensure personnel receive the resources they need but are excluded from resources that are outside of their needs.

#### **Boundary Protection and Event Management for Managing the Security Lifecycle** – is:

- Sometimes referred to as SIEM (Security Incident Event Management),

- Developing a stringent process for identifying, reporting, and responding to encountered cyber threats in an appropriate manner, from Near Real-Time to a scheduled approach.
- Implement a process that safeguards the enterprise while adhering to audit, documentation, quality, and risk management guidelines that ensure compliance with FISMA, OMB, and other government regulatory requirements.

### CDM Three Phase approach project flow

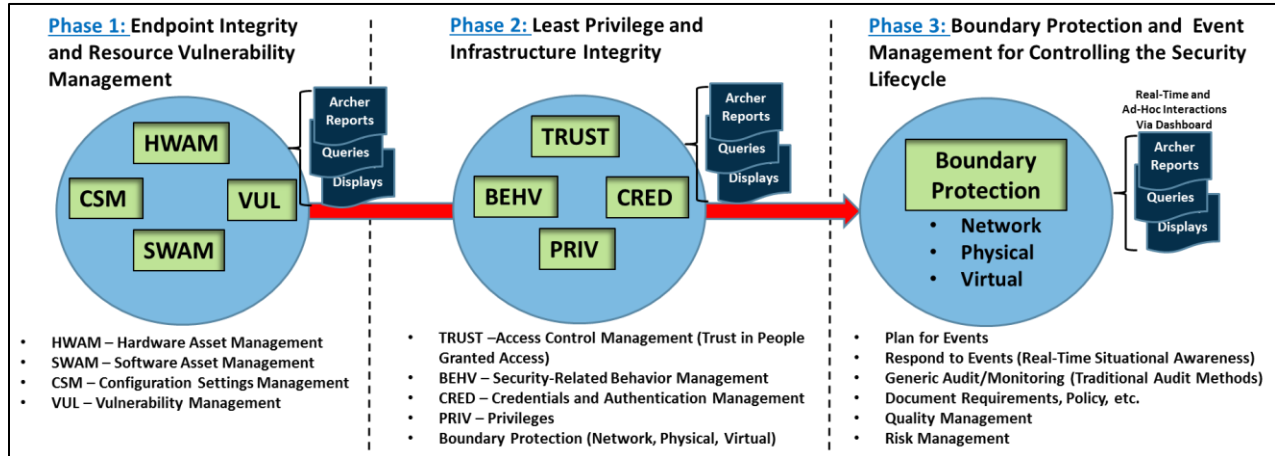


Figure 2: Overview of the CDM Dashboard System's Three Phases

Phase 1: Endpoint Integrity and Resource Vulnerability Management

Phase 2: Least Privilege and Infrastructure Integrity

Phase 3: Boundary Protection and Event Management for Controlling the Security Lifecycle

## Video

Link to CDM Videos and related information



## Application Development and Data Sensitivity

Computers process applications that represent a product or a service. A business exists to sell products and services, so the business would want to protect their investment as well as possible. Academic and industry professionals designed approaches that became Best Practices. They included:

1. **COSO** (Committee of Sponsoring Organizations) to develop Risk Management and Mitigation Guidelines throughout the industry.
2. **CERT – RMM** - CERT Risk Management Framework and Risk Maturity Model.
3. **RMF** – Risk Management Framework
4. **CobIT** (Control Objectives for Information Technology) to Plan and Integrate business directions and goals within the IT Environment. CobIT phases consist of:
  - a. Business Objectives
  - b. Information
  - c. IT Resources required.
  - d. Planning and Organization
  - e. Acquisition and Implementation
  - f. Delivery and Support
  - g. Monitoring and Reporting
5. **ITIL** (Information Technology Infrastructure Library) version 3 – provides a five-phase approach to supplying and servicing applications, including:
  - a. Service Strategy
  - b. Service Design
  - c. Service Transition
  - d. Service Operations
  - e. Continual Service Improvement.
6. **CMMI** (Capability Maturity Model Integration) provides a three-phase approach to optimizing the maturity of your enterprise through:
  - a. Overview of CMMI Solutions for Development, Services, and Acquisitions
  - b. Process Areas for Acquisitions, Development, and Services
  - c. Core Processes for sixteen areas of concern.
7. **GRC** (Governance, Regulation, and Controls) Adherence to Compliance Laws and Regulations
8. **Supply Chain Management**
9. **Systems Management Disciplines and Workflow**
10. **Systems Management Organization**
11. **SDLC** (Systems Development Life Cycle)
12. **Data Sensitivity**
  - a. Business Purpose of Data
  - b. Ownership and Stakeholders of the data
  - c. Sensitivity Level of the data
  - d. Criticality, Sensitivity, and Usage of the Data (CRUD)
  - e. Access Controls and security Requirements for the Data
  - f. Back-up, Archive, and Recovery requirements

See Appendix ‘A’ for more details regarding these topics.

## Network Access

Networks connect end users to computer services via Local Area Networks (LAN), Wide Area Networks (WAN), Virtual Private Networks (VPN), or the Internet via the World Wide Web (WWW).

In System Network Architecture (SNA) terms, the user location is a Physical Unit (PU), and the Application is a Logical Unit (LU). The PU and LU Bind during a Session. If the Bind is broken (say a communications line does down), you can rebind the session through an alternate path – if available. This weakness led to the need to eliminate any Single-Point-Of-Failures associated with critical resources. Correcting problems through a series of Operator Commands (i.e., unbind, shut down, de-allocate, re-allocate new path, bring up, rebind) became the norm. Eventually, Operator Command sequences became Macros that automatically executed when an error condition occurred. This process has grown into a highly effective way of controlling the enterprise environment.

Today, Domain Name Services (DNS) define the users within a Domain by name and Physical Assets by IP (Internet Protocol) Address. Since Operating Systems are name driven, they present a name to the DNS, which returns an IP Address for the asset. The Domains name allows a user to log on to a specific Domain to perform their tasks. With the advent of Virtual Systems, the use of domains has become more important.

Domains define the Virtual Instance location where you are running the application from, including Development, Testing, Acceptance, Production, and Recovery domains. Instances contain all the resources associated with a Domain (i.e., Storage, Computer, and Network). This helps track the application System Development Process from conception to recovery. The application's name remains the same, but the IP (Internet Protocol) Address of its components will point to the environment domain where it is processing. Domain names support specific types of work, or groups, within an enterprise so that work can be segmented to achieve greater protection.

Lately, the need to integrate security, encryption, cryptography, and entitlements has led to Personal Identification Verification (PIV) cards that prove an individual's identity. An individual's Biometrics (e.g., Finger Prints, Iris Scans, Facial Recognition, etc.) are stored in a smart card chip and in a personnel database when registered. A Live Scan of PIV card biometric information compared to the Chip Information and Database record is required to verify a person's identity. A positive comparison is required for access to the physical or logical assets you desire. The government employs the PIV card, and a PIV-I (Interoperability) card is for government contractors or for business enterprises. Together, they are a Unique Universal Identification Card (UUID) used to verify a person's identity for all ranges of requirements.

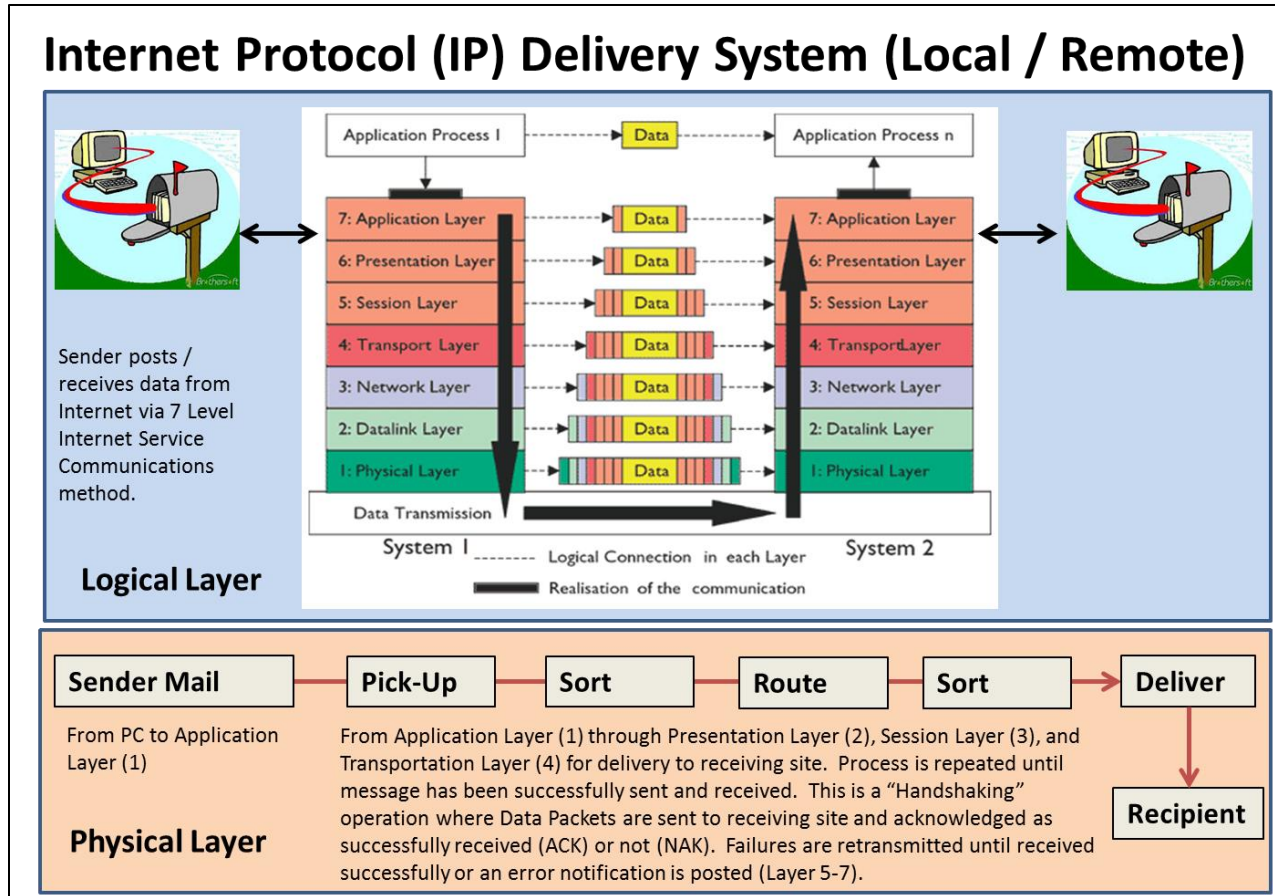


Figure 3: Internet Protocol (IP) Delivery System (Local / Remote)

### Recovery Operations using Domains.

If the User Name and IP Address are the same and the domain component names remain the same across domains, then changing from one domain to the other is transparent to the end user. They are still requesting components by name; the Domain Name Server for the Domain is simply pointing to a new area with the same name in the Domain's environment. Using this approach allows the user to stay in one place, while operations are migrated from one domain to another. In the case of recovery, this allows the user to experience a disaster event and not even know it occurred. No loss of data through Store-And-Forward and the application name stays the same in the recovery environment. This is the goal of an Active / Active environment, but it requires the Production and Recovery Domains to be active and data to be synchronized. A Recovery Point Application (RPA) is used to produce checkpoints every defined time (i.e., 5 minutes, 1 hour, etc.) and a Forward Recovery (FR) file is used to load data from the last checkpoint to the last successful operation. Store-And-Forward stops the failing operation. The last operation reinitiated upon recovery will pick up right where operations left off.

### Logon to a Domain with today’s security protection

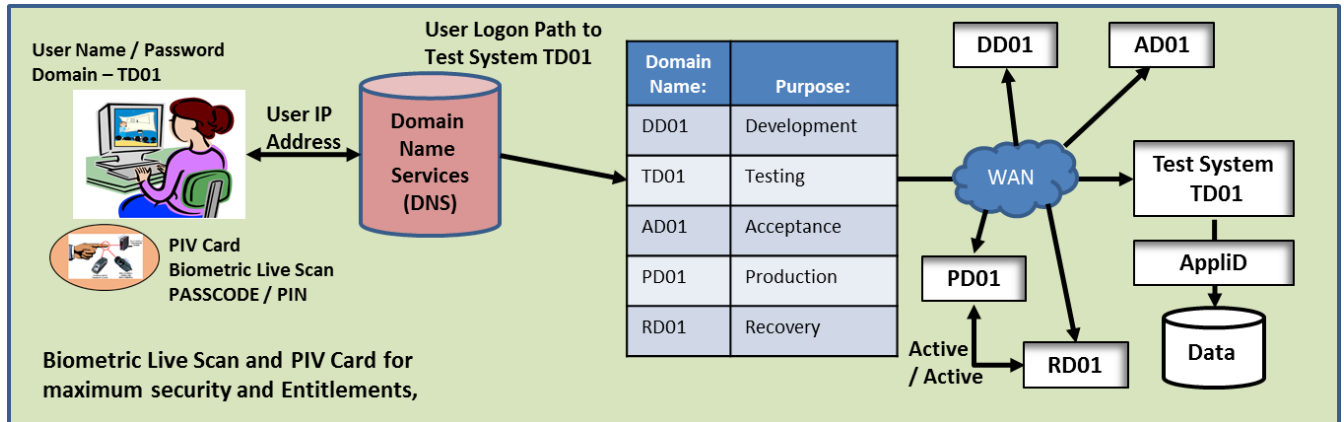


Figure 4: Logging on to a Domain with the latest security precautions.

Users have a User id and Password. Enhanced security provided by a PIV card and live biometric scan verifies a person’s identity and grants access to physical and logical resources. The Domain name segments work by user authority, entitlement, and associated work group.

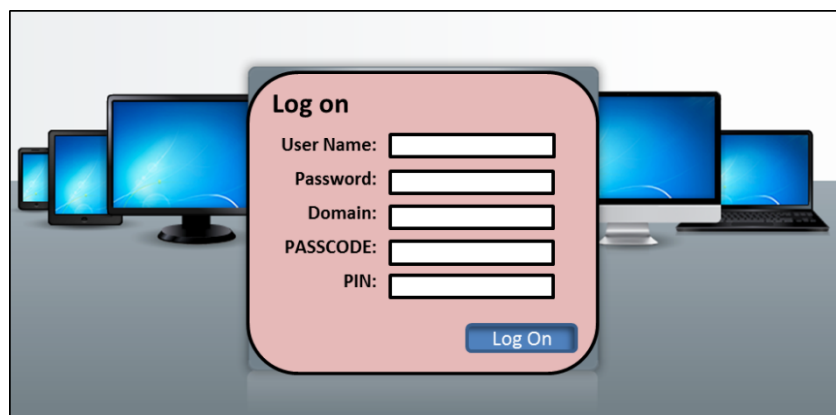
The Systems Development Life Cycle (SDLC) allows migrating an application from one domain to another along the path needed to become a Production Application. A Recovery Domain synchronizes the Production Doman to support Disaster Recovery operations, providing an Active / Active environment for immediate recovery and a Failover / Failback environment for fast recovery.

This represents the foundation for today’s Best Practices in building and protecting enterprise resources.

To simplify the access process a Log On screen provides entry to a Domain by a User.

### The Logon Process

Figure 5: The Logon Function of Applid, Userid, Password (with a Domain Passcode included)



## Building and Protecting the Environment

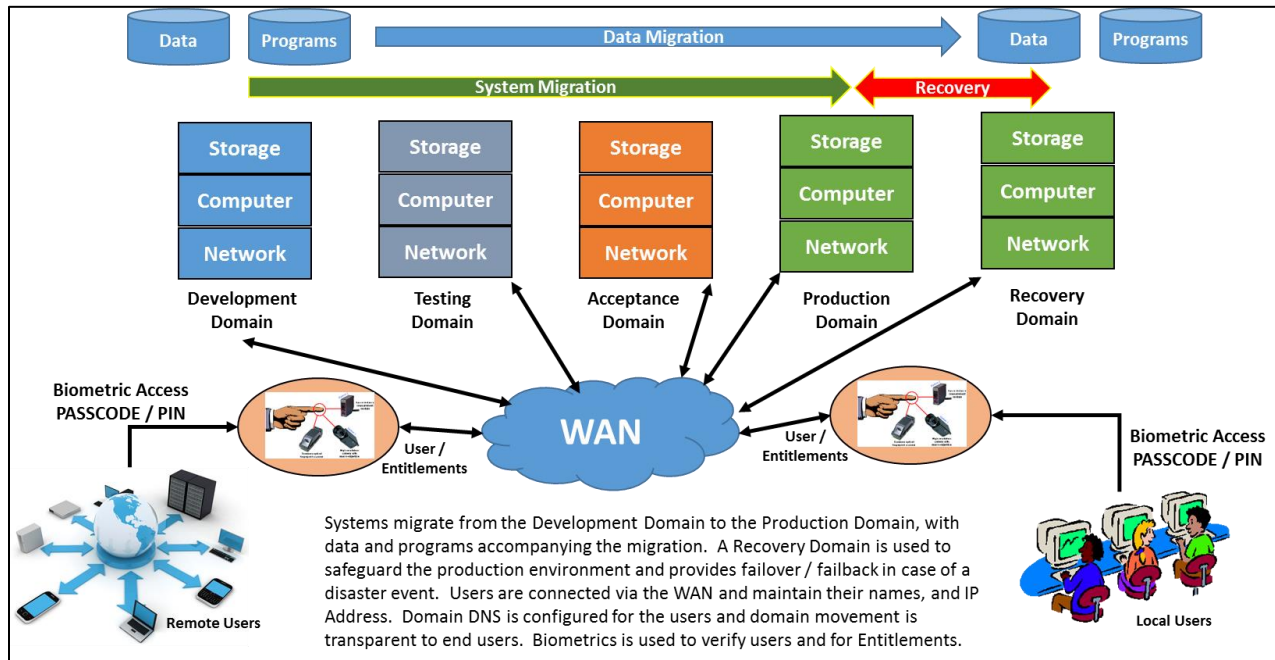


Figure 6: Domain workload segments and recovery operations.

Applications are migrated from the Development to the Production Environments, with a Recovery Environment provided to protect against disaster events. Users must provide verification through a biometric live scan to gain access to their entitled resources.

### What is required to protect our enterprise and society?

Obviously, protecting our computerized world is a prime directive for society to continue to move forward. Could you imagine a world without Google, or Facebook, or email and Instant Messages? Heck, people would have to talk to each other again face-to-face and everything presently controlled with the help of a computer would be controlled and serviced manually.

Past attempts at computer security have provided a foundation to move forward and protect our computerized resources, but it only takes one “really big” virus to infect thousands of computers, so we have to be vigilant and constantly aware of “**New Day**” threats (i.e., those threats that have yet to be experienced). The sheer volume of computerized traffic has surpassed man’s ability to monitor and mitigate threats already, so now tools safeguard against threats. These tools include:

1. Intrusion Detection (who is entering the system and from where)
2. Firewalls (are they allowed entry and access to requested resources)

3. Anti-Virus and Anti-Malware systems
4. Persistent vector attacks named PEN attacks that are sneaky, flexible, and able to learn.
5. SEM - Security Event Management (Access Logs)
6. SIM - Security Information Management (Data Usage Logs)
7. Security Event Information Management (SIEM), combining SEM and SIM
8. Security Analytics to evaluate Risk Impact
9. Role Based Access Control (RBAC) systems and Entitlements.
10. Threat Management
11. Risk Management
12. GRC – Governance, Regulations, and Compliance
13. Disaster and Business Recovery Management (BCM - Business Continuity Management)
14. Enterprise Resiliency (combining Recovery Teams and Tools)
15. Corporate Compliance (insuring adherence to laws and regulations for all countries where your enterprise conducts business)

### What are we protecting?

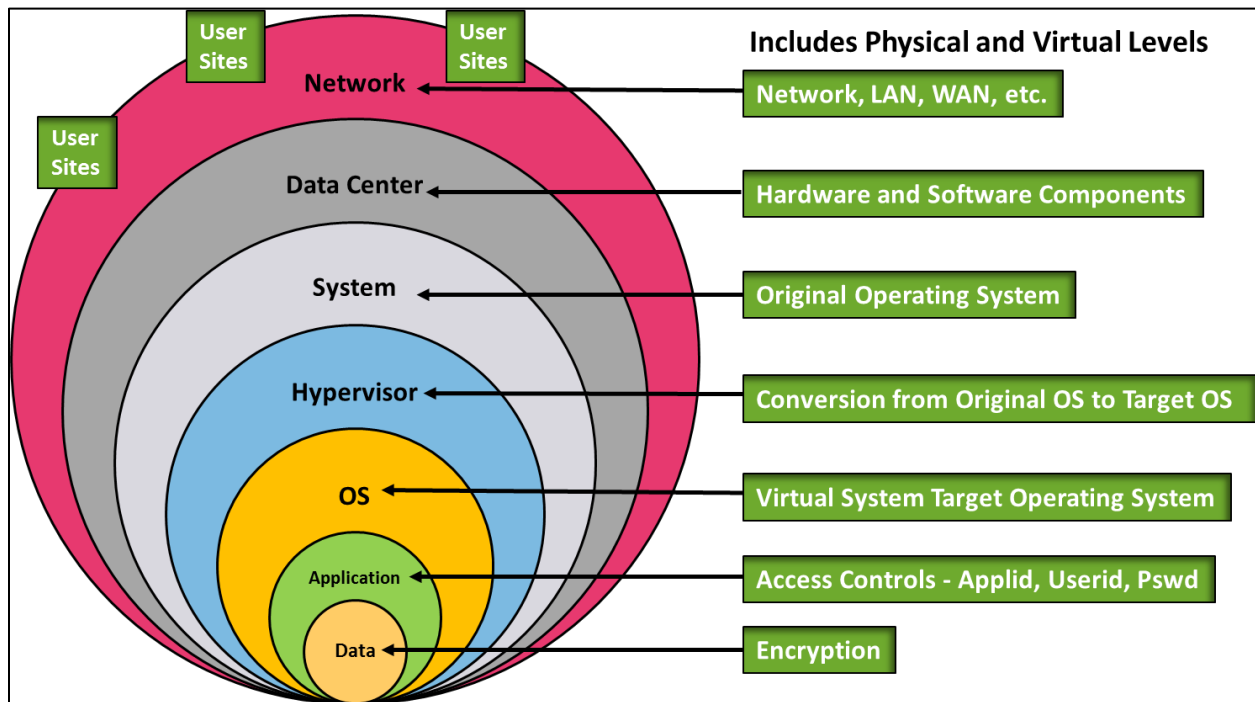


Figure 7: Protecting Enterprise Data from outside intrusion with layers of protection.

### SIEM – Security Incident Event Management

The list of security tools can go on forever, but we are now at a point where we can detect, record, and track security events from the user endpoint, through the network, to the computer. Unfortunately, we are not humanly able to analyze the vast amounts of data presented. We need help doing that in the

form of the SIEM (Security Incident Event Management) and Security Analytics approach, combined with Security Visualization.

## SA - Security Analytics

Security Analytics (SA) has evolved over time as described below.

1. **Initially** security management was concerned with perimeter defense and relied on Physical Security in the form of Guards, Locked Doors with Key Passes, and fenced off areas that evolved into concentric circles around critical resources. These defenses were Security Event Management (SEM) for area access categories that were prevalent at the time.
2. **The second phase** of security management was Security Information Management (SIM) and incorporated logical precautions as dictated by Compliance Laws and Regulations. These requirements, initially developed by the enterprise, later became government and industry requirements. Over time, the volume and time requirements associated with compliance resulted in the need for a better way of detecting and responding to security events that impact information.
3. **The current phase** of security management incorporates methods for visualizing security events, and information impacts, named Security Incident Event Management (SIEM), which is a rapid method for examining security logs to detect and repair known security incidents, while identifying new events and reporting them to the proper authorities. With the use of Big Data Analytics and Visualization techniques, the newly established Security Operations Center (SOC) could best identify, rate, and respond to flaws that posed cyber and technology threats.

For Security Analytics to succeed, it is necessary to implement tools and procedures capable of quickly responding to security intrusions in near real-time. Without SA tools, the enterprise would have a challenging time defending itself against hackers and cyber-attacks because of volume and diagnostic times.

## SOC - Security Operations Center

Ideally, we could use a Security Operations Center (SOC) that can monitor and display all security related events through dashboard screens that are color coded and equipped with thresholds and alarms to alert us of unauthorized activity or potential threats. This is in process today with improvements constantly made to include machine learning and artificial intelligence, so that lessons learned can be instantly applied to the goal of detecting and mitigating security and technology threats in near real-time. This technique is Continuous Diagnostic and Mitigation (CDM). Today, the private and public sectors are moving toward integrating CDM into their environments.



Figure 8: Security Operations Center (SOC)

### Key Characteristics of SIEM and SA Platforms

Key Characteristics of Security Incident Event Management (SIEM) and Security Analytics (SA) Platforms	
Characteristics:	Description:
Speed of Transaction Analysis	The ability to analyze a threat event and return a decision about it in near real-time, leading to an automated security control system.
Amount of Data Analyzed	Petabytes requiring Big Data tools to analyze and report on encountered error conditions and their mitigations.
Big Data Infrastructure	Because of the diversity and volume of data, it is necessary to utilize Big Data systems to analyze information.
Event Correlation Process	Context-based, adaptive, and risk-based threat detection.
Integrated Platform	Platform must include the ability to capture network analysis and visibility (NAV), threat intelligence, Security User Behavior Analysis (SUBA), and SIM data to then present that information to authorized consoles
Machine Learning	Supervised and unsupervised machine learning methods detect anomalous behavior without the need for pre-written rules.
Risk Computational Models	Statistical-based and rules-based risk and security event modeling
Entity and Link Analysis	Entity and Link Analytics - evaluating network, host, and endpoint devices linked together
Statistical Probability Methods	Probability models to determine the likelihood of a breach

Figure 9: Features of a SIEM and Security Analytics System

### Role Based Access Controls (RBAC) and Entitlements

The technology growth in the security field is spectacular, but it still needs input from man to know who is using the system and what their authorization is, based on their job title and functional responsibilities (**Role Based Access Control**). RBAC is associated with the resources (both physical and logical) that an individual is **Entitled** to use to satisfy their current functional responsibilities. If they leave the organization, or change functional responsibilities, then their level of entitlement changes to reflect their new needs, so RBAC and Entitlements are a key part of security, but how about a person’s behavior? We all know people who have suffered life-altering experiences, even disgruntled employees who are unhappy with their job, the company, or management. Sometimes these people can inflict worse harm than a Hacker can, and precautions should be included in your security management system, otherwise you may have to contend with a saboteur or active shooter situation.

As you can see, implementing an enterprise-wide security management system can be an exceedingly challenging task, but one whose goals meet the Business Continuity Management needs for today’s enterprises. You can also derive a two-prong approach to security management, one based on technology improvements and the other based on personnel management. Although technology and personnel are different disciplines, it is hard to assign security controls that allow people access to what



they need if you do not know their entitlements, as defined in their functional responsibilities. Hence, implementing a security management system requires an enterprise to have personnel and technology work together to achieve successful results. Of course, Legal, Risk Management, Compliance, and Auditing must all have seats at the table to define your vulnerabilities, rate them on criticality, and prioritize their resolution.


### Continuous Diagnostic and Mitigation (CDM) System

One of the most aggressive methods employed to overcome security problems is the CDM system. Designed to capture and mitigate cybercrimes and technology threats in near real-time, CDM employs Scanner and Sensor Management to deploy Scanners and Sensors that are Rule Driven and able to mitigate known technology threats (i.e., vulnerabilities, configuration errors, patches, etc.) and cybercrimes (known fixes for malware, virus, Trojan horses, etc.). When scanner and sensor results return errors an automated Risk Analysis is performed to rate them from worse to least bad. Technical resources repair errors in descending order from worse case down, thereby eliminating cybercrimes and technology risks based on their potential impact.

### Continuous Diagnostic and Mitigation (CDM) project overview

**The goal of a Continuous Diagnostic and Mitigation Dashboard Project is to:**

- **Provide** a **Continuous Diagnostic and Mitigation (CDM) Dashboard System** that communicates cyber-crime and technology threats and Error Detection information between the Enterprise Security Operation Center (SOC) and the end user **through these five steps:**



- **Collect** - via a set of sensors and collection devices (Network based Firewalls, Intrusion Detectors, Access Rules and Controls, and SIEM (Security Information Event Management)) and tools collectively known as the Network Dashboard;
- **Process** - the collected information is compare with Sensor and Scanner Rules to determines if security policies have been violated and are also used to identify risk information and filter non-threat information,
- **Provide** - a Summary Reports to Enterprise Management and distribute the report to end points and department heads on a periodic basis (at least every 72 hours), or on-demand;
- **Analyze** - **Threat and Defect information** to provide the department heads and end points with a **Threat Report** consisting of sorted **"Worse Case" Threats by priority of impact;**
- **Use to** - **coordinate a Threat Response** by all Departments / Agencies, in **"Worse Case"** order, so that all pertinent information needed to address the **"Root Cause"** of the threat and reduce / eliminate the **"Threat Impact"** can be acted on.

- The Enterprise must define **Entitlements** associated with Personnel Job Functions, so that a **Role Based Access Control** (RBAC) security system can be implemented.

Figure 10: The Goals of a Continuous Diagnostic and Mitigation (CDM) Dashboard System

The CDM process has proven to be a very efficient method for uncovering and correcting potential risks. Using a Dashboard to display error reports and environment operations enhanced the use of CDM.

Beyond correcting cybercrimes and technology risks, CDM also provides Role Based Access Controls (RBAC) to support Entitlements related to a job title. Personnel behavior is also included in the CDM system to provide total protection for an enterprise. Integrating a CDM system within an enterprise can provide compliance, risk management, error analysis, and disaster recovery support. CDM is a rapid method for controlling your enterprise and an easy to implement and tailor to your needs.

## How should an enterprise implement their security management system?

Like any other major project, there are specific phases to achieve to implement the best security management system for your enterprise. The basic phases are:

- 1. Requirements Definition to define what your security system should protect, including:**
  - a. Resources like facilities and assets within a facility'
  - b. Personal Identification Verification (PIV) smart card to identify individuals and their certifications for accessing locations and assets (PIV cards are for government enterprises and PIV-I (Interoperable) cards are for business enterprises. These cards are also Universal Unique Identification (UUID) Cards),
  - c. Derived PIV Card (DPC) which provides Mobile Devices with a Token like PIV card,
  - d. Entitlements to critical locations and assets based on Job Title.
  - e. Guards and Key Card access readers to control access to physical locations and logical assets,
  - f. Audit Trail for recording and tracking security related events,
  - g. Logs and Analysis Tools to identify security violations and rate them by Risk Impact,
  - h. Reporting via thresholds, color coded alarms, alerts to notify personnel, actions to be taken (either manually or via automated responses), and event management.
- 2. Needs Analysis – to fully define all your enterprise's protection and compliance needs, including:**
  - a. Physical and Logical needs (i.e., Physical Access System, Logical Access System).
  - b. Critical Systems and Resources.
  - c. Network, Computer, and storage management considerations, both physical and virtual.
  - d. Enterprise Resiliency and Corporate Certification.
  - e. Risk Management and Insurance.
  - f. Business Continuity Management; and,
  - g. Human Resource Management and Information Technology.
- 3. Architectural Diagrams**
  - a. Physical Environment.
  - b. Logical Environment.
  - c. Present vs. Future requirements.
- 4. Engineering Diagrams**
  - a. Present Equipment and Infrastructure.
  - b. Future Equipment and Infrastructure Requirements.
  - c. Roadmap to move from present to future environment.
- 5. Request for Proposal (RFP) issuance**
  - a. Define the needs for assistance in a Request For Proposal (RFP).
  - b. Locate qualified vendors who can provide the needed services and products.
  - c. Forward the RFP to selected vendors and coordinate their responses.
  - d. Select vendors to assist in accomplishing goals.
  - e. Initiate the project by creating a universal Project Plan.

**6. Execute the Project Plan and monitor status.**

- a. Kick-off project.
- b. Monitor and report on status of project.
- c. Make necessary project adjustments.
- d. Accomplish Project Goals.

**7. Integrate Project Deliverables within everyday functions.**

- a. Completely document project results and provide needed manuals.
- b. Along with Awareness Programs from project conception through implementation, deliver Documentation and Training to personnel as needed.
- c. Conduct Training Upgrades as the environment evolves.
- d. Ensure that personnel job functions are included in the new system, so that events are tracked and recorded to ensure adherence to Standards and Procedures.
- e. Conduct periodic reviews and Post Mortems to gain Lessons Learned and develop Teaching Events as needed.
- f. Integrate Support and Maintenance to resolve encountered problems.
- g. Integrate Change and Release Management to implement changes and enhancements to the system in a controlled manner through Version and Release Management.

This seven-step process should get you on your way, but every enterprise is different, and modifications needed to best suit your needs may be required.

**Automated Load Balancing and Error Handling**

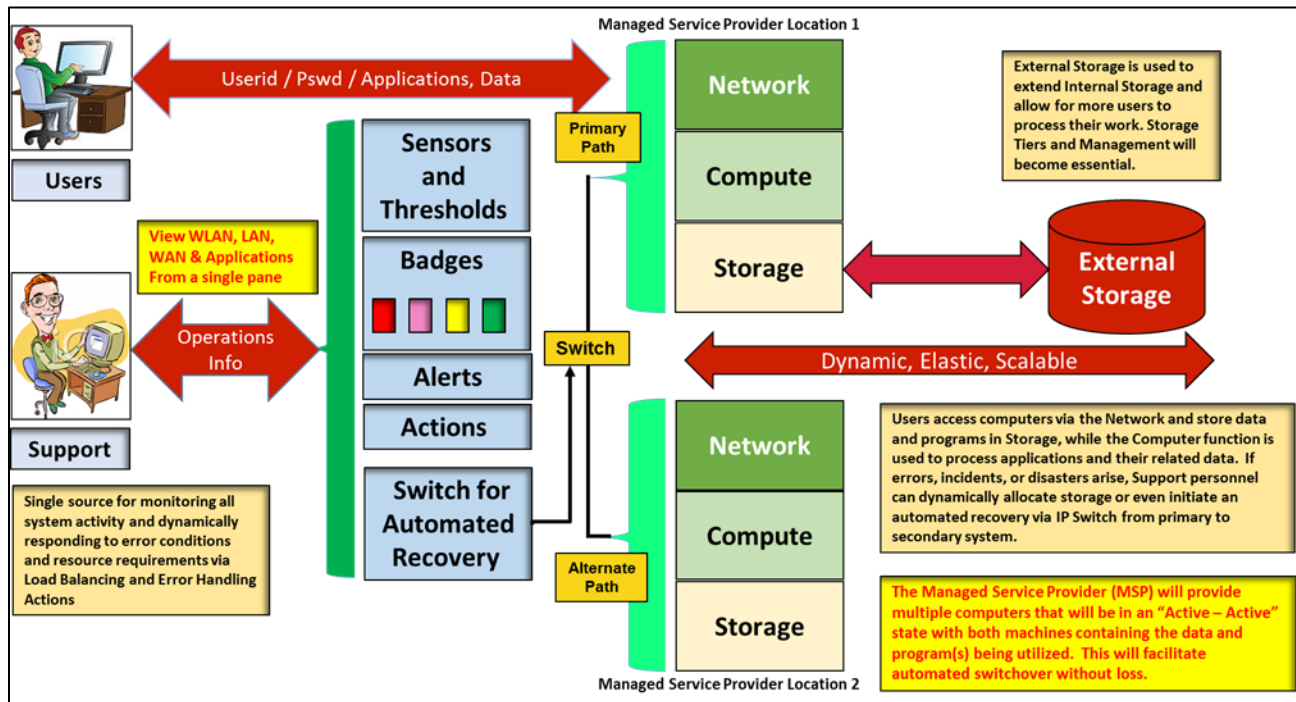


Figure 11: Load Balancing and Error Handling for a Virtual Environment with Automatic Recovery

The Security Operations Center (SOC) responds to encountered errors due to load balancing or error events. Badges are color-coded indicators of error conditions (Red being Bad and Green being good for example). Badges are associated with pre-defined thresholds associated with system loads or error conditions. Alerts occur when pre-defined thresholds are crossed. Alarms generate warnings to technicians and management when thresholds are crossed (going from good to bad or returning from bad to good). Actions respond to Alerts, either manually or through automated responses. This process continues until all error issues are resolved and operations returns to normal load conditions.

Network scanner and sensor rules contain tests for known cybercrimes and technology threats. When scanner and sensor tests return error results, the alert process and rule management initiate responses. Known errors are resolved while new errors are logged for investigation. Error summary reports provide a Risk Analysis producing an Alert Report that lists errors in Worse Case First order. Technicians resolve problems listed at the top of the Alert Report first, and then work their way down the list until all problems are resolved. This technique produces the best results for reducing problem impacts and threats.

The successful implementation of the Continuous Diagnostic and Mitigation (CDM) process aids government and business enterprises.

Load balancing and error handling is included in Virtual Systems that have eliminated all "Single-Points-Of-Failure" and programmed secondary paths as problem circumventions. Active / Active environments will maintain applications and data in-sync across the primary and secondary facility to eliminate any interruption to production operations. This configuration can switch from primary to secondary facility automatically and will be transparent to the end user.

Security management systems integrated within your everyday environment can sense, rate, alert, and take immediate actions to safeguard the enterprise. Safeguarding your enterprise occurs in the following manner:

1. Establish Thresholds to define security categories like Good, Poor, or Bad.
2. Assign color codes to the categories like, Good (Green), Poor (Yellow), and Bad (Red).
3. Develop an Alarm mechanism that will notify the Security Operations Center (SOC) Staff of abnormalities when they occur, both going from good to bad and returning from bad to good.
4. Implement an Alert Mechanism that would notify people when a security flaw occurs or is resolved. This can consist of emails, problem tickets, phone calls, or bells and sirens.
5. Define Actions-to-be-taken for the full range of security violations and associate them to thresholds, badges, and alarms to bypass security/failure conditions and immediately follow-on with necessary repairs and mitigations.
6. Record all activities and follow-on incidents with a Post Mortem discussion to define the reason behind the failure, developing lessons learned and teaching events as needed.

Computers consist of three components, storage, computer, and network monitored and controlled by Load Balancing and Error Handling. Automating these functions leads to a Software Defined Data Center (SDDC) capable of optimizing throughput and minimizing problems.

## Organizational Considerations

Now that you understand the aspects of Security, you know how complicated it can be to implement, maintain, and optimize in an ever-changing business landscape. For that reason, it is important to consider developing an enterprise structure to manage your security requirements. Examples of security management positions are below.

### Chief Information Security Officer (CISO)

Enterprises have elevated Information Security to the 'C' level and announced the creation of a Chief Information Security Officer (CISO). Sometimes individuals who have risen through the security technology ranks and have extensive firsthand experience identifying and resolving security threats become the CISO. In other enterprises, the CISO position is more involved with legal, business, compliance, and issues. The person holding the CISO position can therefore have a wide range of backgrounds and qualifications, but every CISO is responsible for reporting to the CEO on how best to protect resources, intellectual property, reputation, and the confidence of the client base. Other enterprises have addressed both needs by creating a Chief Security Officer (CSO) and a Chief Information Security Officer (CISO), with the CSO reporting to the CISO. This final approach seems to be the most adopted approach used by today's enterprise. Another 'C' level position of importance is the Chief Compliance Officer (CCO) who is responsible for insuring that the enterprise complies with all regulations and laws in the countries where the enterprise does business.

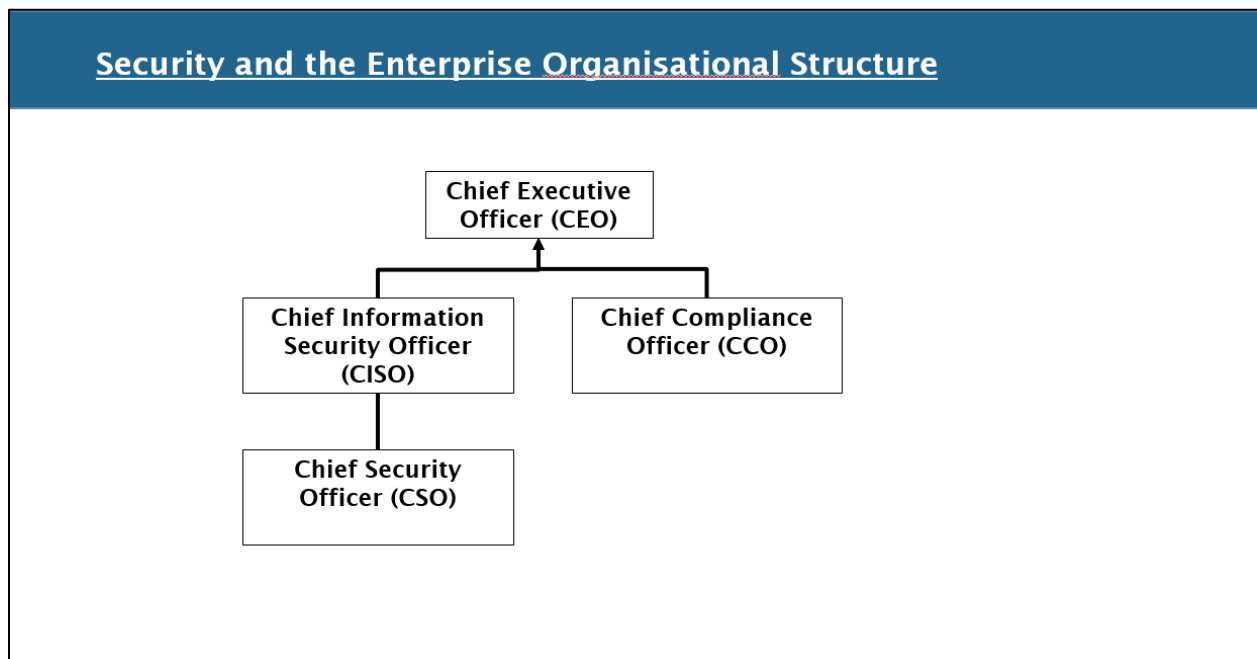


Figure 12: The enterprise security and compliance organizational structure.

## Defining the needs and responsibilities of an Enterprise Security System

First, define the range of responsibilities associated with the enterprise security environment. Then define a Threat Based Approach to implementing security precautions, and finally a Risk Based Approach to implementing security precautions. Security concerns are defined, rated; and evaluated; before you can create functional responsibilities, select tools, define displays, alerts, and actions to mitigate encountered cybercrimes and technology threats. A Continuous Diagnostic and Mitigation (CDM) system is best suited to satisfy the security management needs of the enterprise.

The approach presented here will provide four areas to consider when establishing an enterprise security system to mitigate security and technology threats. They are:

1. Responsibilities included in establishing an Enterprise Information Security Environment
2. Threat based approach to implementing Enterprise Security Management
3. Risk based approach to Enterprise Security Management
4. Cloud Risk and Security Protection

## Defining Security and Technology threats and assigning Responsibilities

### Information Security Responsibilities

Information Security Responsibilities	
<ul style="list-style-type: none"> <li>• Physical Security</li> <li>• Data Security</li> <li>• Intellectual Property</li> <li>• GRC – Governance, Regulation, Compliance</li> <li>• Risk Management</li> <li>• Forensics and Investigations</li> <li>• Business Continuity Management</li> <li>• Data Privacy and Entitlements</li> <li>• Strategic Security initiatives</li> <li>• Audit Universe and Audit Schedules</li> <li>• Threat Intelligence Capabilities</li> <li>• Situational Awareness</li> <li>• Continuous Diagnostics and Mitigation (CDM)</li> <li>• Ownership of Risk and Security in the Cloud</li> <li>• Cyber Threat Intelligence:               <ul style="list-style-type: none"> <li>• Cyber Security National Action Plan</li> <li>• Cyber Security Policies</li> </ul> </li> <li>• Network Security – SIEM</li> <li>• Encryption, Cryptography, and Bio-Metrics               <ul style="list-style-type: none"> <li>• PIV, PIV-I, CAC</li> </ul> </li> <li>• Interfacing with Professional Organizations</li> <li>• Documentation, Awareness, Training, and Certification of staff</li> </ul>	<ul style="list-style-type: none"> <li>• Firewalls, Intrusion Detection, Anti-Virus and Malware</li> <li>• IT Security Tools and Products</li> <li>• Threat Intelligence Capabilities:               <ul style="list-style-type: none"> <li>• Data from Systems, Applications, and Network</li> <li>• Intrusion Detection and Prevention systems</li> <li>• Endpoint Anti-Virus and Security Controls</li> <li>• Firewalls and Anti-Malware</li> <li>• Scanner and Sensor Rules and Results Tracking</li> <li>• Role Based Access Controls (RBAC)</li> <li>• PIV / PIV-I and Entitlements</li> <li>• HWAM, SWAM, Vulnerabilities, and Configuration vulnerability detection and protection of Technical Environment</li> <li>• SPLUNK data collection and analysis tools, et al</li> <li>• Prioritize identified Gaps and Exposure Risks</li> <li>• Unified Security Intelligence Management System combining Log Management, endpoint and network monitoring, SIEM and Security Analysis, Reporting and Mitigation Action Plans</li> <li>• Develop a Three Step Approach:                   <ol style="list-style-type: none"> <li>1. Infrastructure Protection</li> <li>2. Entitlements and staff</li> <li>3. Behavior Analysis</li> </ol> </li> </ul> </li> </ul>

Figure 13: Defining Security and Technology Threats and Assigning Responsibilities

## Approaches to developing an Enterprise Security System

The range of problems faced by an enterprise is extensive. Include the subjects contained in the “Information Security Responsibilities” chart above to identify and rate the components in the Enterprise Security System that you develop to safeguard the intellectual properties and assets of your business.

There are two approaches presented on the following pages, the Threat Based Approach and the Risk Based Approach. Both have merit and use to define the needs of your enterprise. A third topic is included to identify the special needs of companies utilizing Cloud Based services.

### Threat based approach to implementing Enterprise Security Management

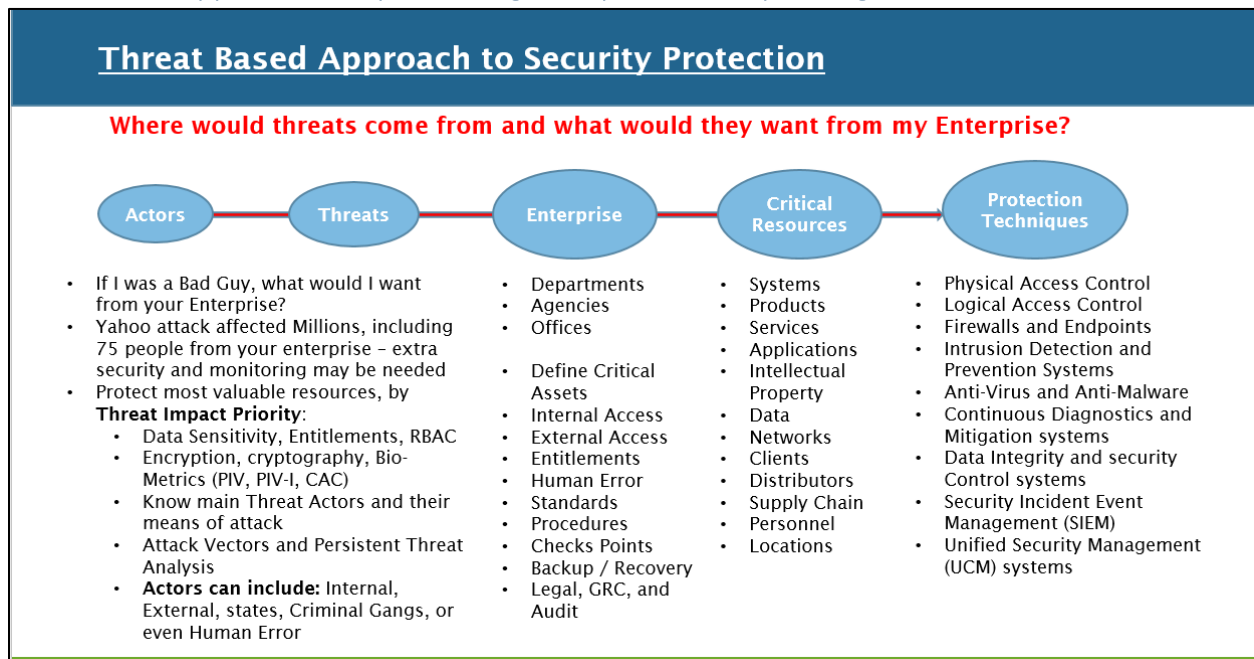


Figure 14: Threat Based Approach to implementing an Enterprise Security System

## Risk based approach to Enterprise Security Management

**Risk Based Approach to Security Protection**

<ol style="list-style-type: none"> <li>1. Rate Asset on a Risk Basis, then Monitor and Report</li> <li>2. Vulnerability Analysis</li> <li>3. Protect the:               <ol style="list-style-type: none"> <li>a. Confidentiality</li> <li>b. Integrity</li> <li>c. Availability</li> </ol> </li> <li>4. Define Risk Impact over the following categories:               <ol style="list-style-type: none"> <li>a. Loss of Intellectual Property</li> <li>b. Loss of Reputation</li> <li>c. Loss of Customer Confidence</li> </ol> </li> <li>5. Formulate Contingencies and Mitigations</li> <li>6. Conduct Risk Analysis of:               <ol style="list-style-type: none"> <li>a. Types of Impacts:                   <ol style="list-style-type: none"> <li>i. Intellectual Property</li> <li>ii. Reputation</li> <li>iii. Customer Confidence</li> <li>iv. Regulatory Compliance</li> <li>v. Financial Loss Potential</li> <li>vi. Likelihood of Occurrence</li> </ol> </li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>b. Rate by Priority and Impact</li> <li>c. Fix Worse Case First</li> <li>d. Start small, then learn, improve, test and repeat</li> <li>e. "Don't let GREAT come in the way of GOOD"</li> <li>f. Improve Standard and Procedures</li> <li>g. Integrate with everyday activities to avoid re-occurrence and reduce exposures</li> </ol> <ol style="list-style-type: none"> <li>7. Develop Risk Visualization displays to better understand and respond to encountered Risks (Dashboards)</li> <li>8. Use Threat Information Feeds and Services based on industry standards like STIX (Structured Threat Information eXchange), or TAXII (Trusted Automated eXchange of Indicator Information), which are easier to share and automate.</li> </ol>
--	--

Figure 15: Risk Based Approach to implementing an Enterprise Security System

## Cloud Risk and Security Protection

**Cloud Risk and Security Protection**

**Cloud Risk and Security Reviews:**

1. The enterprise is still responsible for Risk and Security, even when migrating to the Cloud – including Systems, Applications, and Data.
2. Cloud Service Provider supplied Risk and Security information is limited and not always accurate.
3. Compliance must be reviewed prior to migrating to a Cloud environment (Data Integrity).
4. You must review Legal and Vendor Agreements and Licenses for hidden costs and permissions.
5. In-House security practices may not work in the Cloud and should be scrutinized.
6. Additional Tools, Products, and Resources may be required to continue adherence to security and regulatory requirements.

**Cloud Security Policy:**

1. Clearly identified Executive Sponsor
2. Data Sensitivity and Cloud Data Protection Guidelines must be developed and adhered to.
3. Compliance mandates must be identified and adhered to.
4. Document Cloud Risk evaluation process and results, then obtain sign-off on results or corrective actions.



## Ten Recommended Network Security Tools

Name:	Link:	Use;
Nessus Home	<a href="http://www.tenable.com/products/nessus-home">http://www.tenable.com/products/nessus-home</a>	Assess and evaluate existing security using security scanners and vulnerability assessment tools.
Virus Total	<a href="https://www.virustotal.com">https://www.virustotal.com</a>	Free, on-line Virus scanning tool and a subsidiary of Google
Secunia PSI	<a href="https://www.secunia.com/vulnerability_scanning/personal">https://www.secunia.com/vulnerability_scanning/personal</a>	Regularly scans for Patches that can upgrade your protection and reduce vulnerabilities
Autoruns	<a href="Http://technet.microsoft.com/en-us/sysinternals">Http://technet.microsoft.com/en-us/sysinternals</a>	Scans system for apps included in system at launch and eliminates any not needed apps.
CrowdInspect, Should I Remove It? & Solutio	<a href="https://www.team-cymru.org/Services/MHR/">https://www.team-cymru.org/Services/MHR/</a> <a href="https://www.mywot.com/">https://www.mywot.com/</a> <a href="http://www.crowdstrike.com/crowdinspect/">http://www.crowdstrike.com/crowdinspect/</a> <a href="http://www.shouldiremoveit.com/">http://www.shouldiremoveit.com/</a> <a href="https://www.solutio.com/">https://www.solutio.com/</a>	<p>CrowdInspect, Should I Remove It? and Solutio</p> <p>Knowing what a program is that is running on your computer can be a challenge. What is it? What does it do? Is it malicious? Do I even want it? Should I remove it? Answers to these questions are not too far away. There are tools that can help in this regard, my favorites are: CrowdInspect, Should I Remove It? and Solutio.</p> <p>CrowdInspect pulls data from VirusTotal, the Malware Hash Registry (MHR) (<a href="https://www.team-cymru.org/Services/MHR/">https://www.team-cymru.org/Services/MHR/</a>), WOT (Web Of Trust) services (<a href="https://www.mywot.com/">https://www.mywot.com/</a>), and from its own monitoring of malicious injection activities. With this range of detail, you can quickly discover unwanted operators on your system. Visit: <a href="http://www.crowdstrike.com/crowdinspect/">http://www.crowdstrike.com/crowdinspect/</a>.</p>

		<p>Should I Remove It? focuses on detecting unwanted software, such as adware, spyware, toolbars, malware, and unwanted applications. In the pursuit of removing bloatware and crapware, this tool quickly identifies those applications you want of your system fast. Visit: <a href="http://www.shouldiremoveit.com/">http://www.shouldiremoveit.com/</a></p>
ShieldsUp	<a href="https://www.grc.com/">https://www.grc.com/</a>	<p>ShieldsUp is a free online service for evaluating your Firewall to determine your online exposure. ShieldsUp operates from the Gibson Research Corporation's website (<a href="https://www.grc.com/">https://www.grc.com/</a>) and offers a quick assessment of your attack surface as exposed online. Go assess your system and find out what hackers can see when their network scans your IP address. Follow the recommendations to improve your security and lock down your vulnerabilities. The ShieldsUp service is at <a href="https://www.grc.com">https://www.grc.com</a> in the Services menu.</p> <p>While at GRC, you might want to explore the other amazing tools and services, such as DNS benchmark, HTTPS Fingerprinting, and SpinRite.</p>
Malwarebytes and HijackThis	<a href="https://www.malwarebytes.org/">https://www.malwarebytes.org/</a> <a href="http://www.hijackthis.com/">http://www.hijackthis.com/</a>	<p>Often your anti-malware scanner is not enough. Using advanced supplemental tools to detect and remove malicious code is an essential part of being an Internet user. Two great tools to have on hand are Malwarebytes and HijackThis. These tools can usually operate on your system concurrently with an existing real-time anti-malware scanner present, a feature in malware products do not have. Whenever you suspect an infection or if you think you have inadvertently performed a risky activity, and your anti-malware scanner is staying suspiciously quiet, run one of these tools to discover if your fear is justified.</p>


		<p>Malwarebytes is available at:  <a href="https://www.malwarebytes.org/">https://www.malwarebytes.org/</a>.</p> <p>HijackThis is available at:  <a href="http://www.hijackthis.com/">http://www.hijackthis.com/</a>.</p>
<p>NoScript and ScriptSafe</p>	<p><a href="http://noscript.net/">http://noscript.net/</a></p>	<p>Surfing the Internet has become a dangerous activity. If you are using a Web browser with default configuration, you are vulnerable to a wide range of exploitations and attacks. Issues are because Web sites transmit mobile code to Web browsers for client-side execution. While this code is safe and benign, there is no way for an end user to know when malicious mobile code is being offered until it is too late (i.e., it is already running on the user's system). The only way to mitigate this risk is to disable client-side execution of scripts and mobile code. While done in most browsers directly, it can be difficult, and it usually applies universally. A better solution is to use a browser extension that adds quick access to a range of features including being able to target the settings on a per site basis. For Chrome users, the tool ScriptSafe is a smart choice. For Firefox users, the tool NoScript (<a href="http://noscript.net/">http://noscript.net/</a>) is the clear leader. These tools can be quickly located in their respective browser's extension/add-on marketplace.</p> <p>Note: If you are using a different browser, switch to Chrome or Firefox.</p>
<p>CCleaner</p>	<p><a href="https://www.piriform.com/ccleaner">https://www.piriform.com/ccleaner</a></p>	<p>Just using your computer will cause a plethora of debris to build up over time. This includes temporary files, histories, cached content, cookies, downloads, MRU (most recently used) listings, orphaned files, and stray registry entries. File code remains when uninstalling legitimate or malicious software. From time to time, performing a deep cleaning of your OS will result in improved performance. Try this tool from time to time to maintain performance.</p>

<p>Pandora Recovery</p>	<p><a href="http://www.pandorarecovery.com/">http://www.pandorarecovery.com/</a></p>	<p>Sometimes files get deleted by mistake. Important files. Files that you do not have backed up (you have a backup, right?). Fortunately, the standard deletes function removes the direct listing and pointers to storage clusters, while leaving the actual file data in place. If subsequent writing activities overwrite these "available" clusters, the data is lost. However, if you can attempt a reclamation of the lost file before the data is lost, the act of undeleting may be possible. Try it yourself:</p>
<p>WDO – Microsoft Windows Defender Offline</p>	<p><a href="http://windows.microsoft.com/en-us/windows/what-is-windows-defender-offline">http://windows.microsoft.com/en-us/windows/what-is-windows-defender-offline</a>.</p>	<p>Sometimes your system is infected by something that your native or standard detection and removal tools are unable to address. When you think you are in this situation, before giving up low-level formatting or replacing hardware, try an offline scanner. Microsoft's Windows Defender Offline (WDO) scans your system while the OS is not active. This can give the security scanner the boost it needs to detect and remove the nastiest forms of malware. Download WDO and install it on a spare USB drive, so you can be prepared:</p>

## Appendix 'A'

### COSO – Committee of Sponsoring Organizations (Risk Management Guidelines)

# COSO Risk Assessment



**Committee Of Sponsoring Organizations (COSO)** was formed to develop Risk Management and Mitigation Guidelines throughout the industry.

Designed to **protect Stakeholders** from uncertainty and associated risk that could erode value.

A **Risk Assessment** in accordance with the COSO Enterprise Risk Management Framework, consists of (see [www.erm.coso.org](http://www.erm.coso.org) for details):

- Internal Environment Review,
- Objective Setting,
- Event Identification,
- Risk Assessment,
- Risk Response,
- Control Activities,
- Information and Communication,
- Monitoring and Reporting.

Creation of **Organizational Structure**, Personnel Job Descriptions and Functional Responsibilities, Workflows, Personnel Evaluation and Career Path Definition, Human Resource Management.

Implementation of **Standards and Procedures** guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

**Employee awareness** training, support, and maintenance going forward.

Figure 16: COSO - Risk Assessment Best Practices

First start by identifying your risk and rating risk by priority and impact. This “Best Practice” is well documented and will help you get started building a better enterprise.

CobIT – Control Objectives for Information Technology (Converting Business to IT)

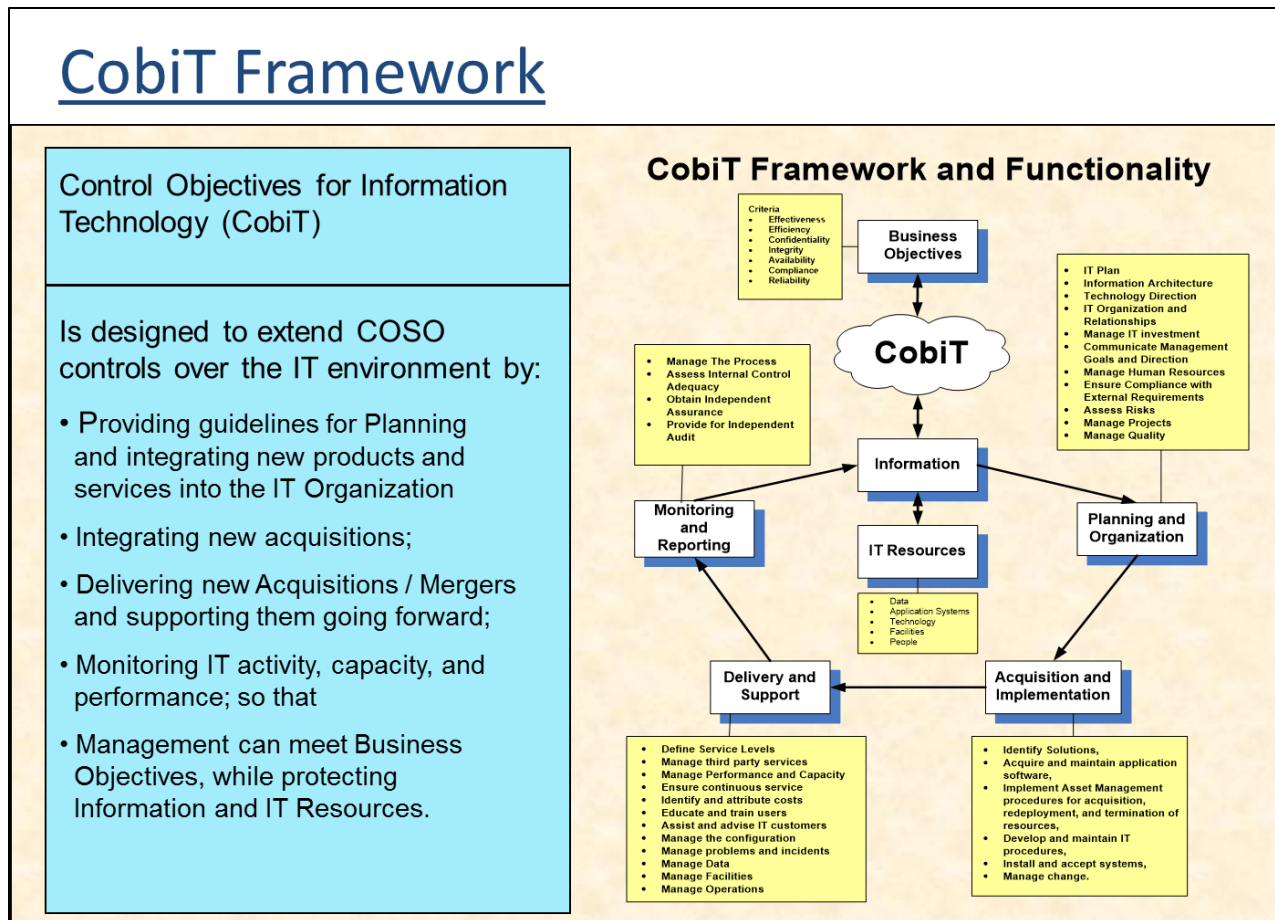


Figure 17: CobIT Framework - Control Objectives for Information Technology

You will have to convert business goals and directions into Information Technology practices and CobIT will provide a pathway for achieving that goal. CobIT is a “Best Practice” and well documented.

ITIL – Information Technology Infrastructure Library (Service Delivery and Support0

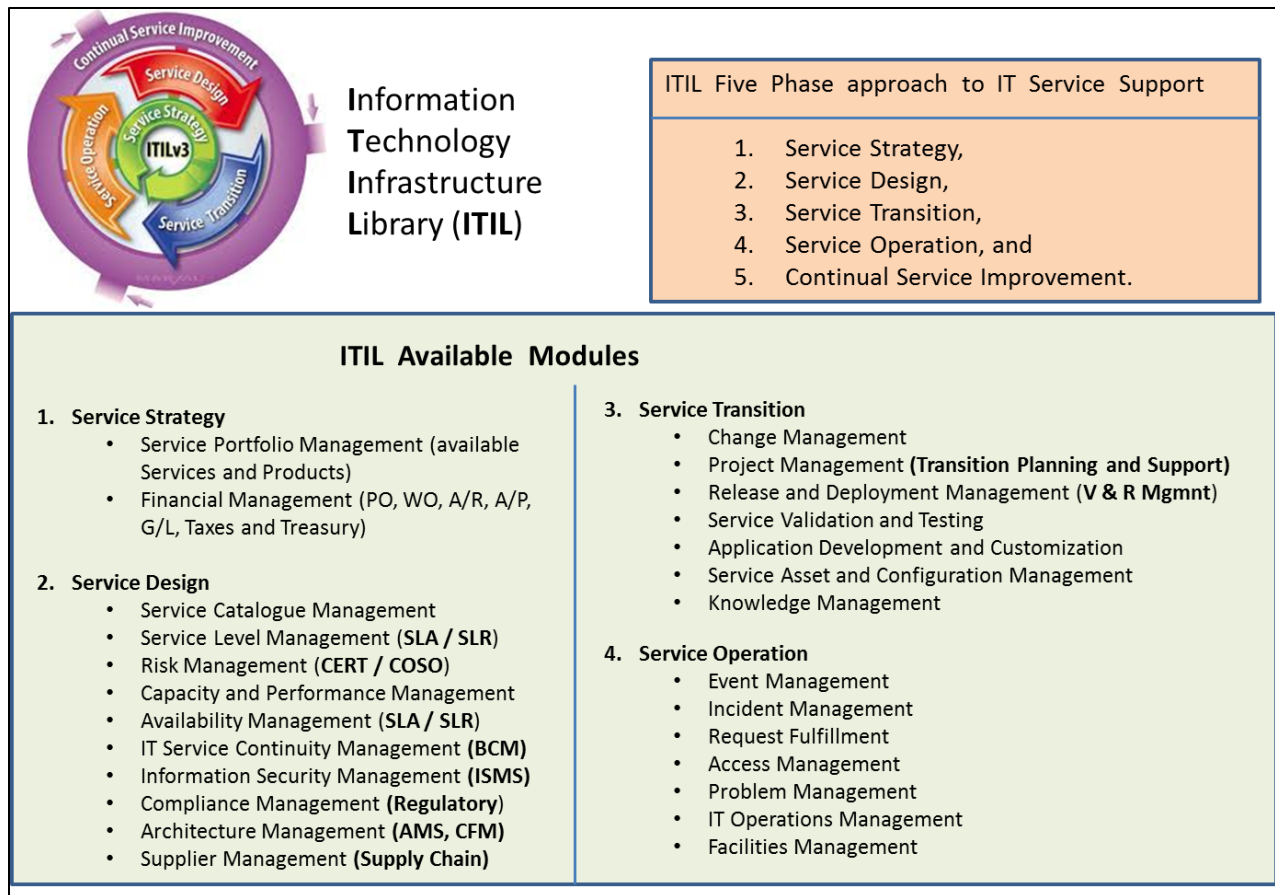


Figure 18: ITIL v3 - Information Technology Infrastructure Library

ITIL is the leading “Best Practice” tool for delivering Information Technology Systems and Support Services. ITIL will provide a solid control process that will optimize enterprise operations.

CMMI – Capability Maturity Model Integration (Optimizing Performance)

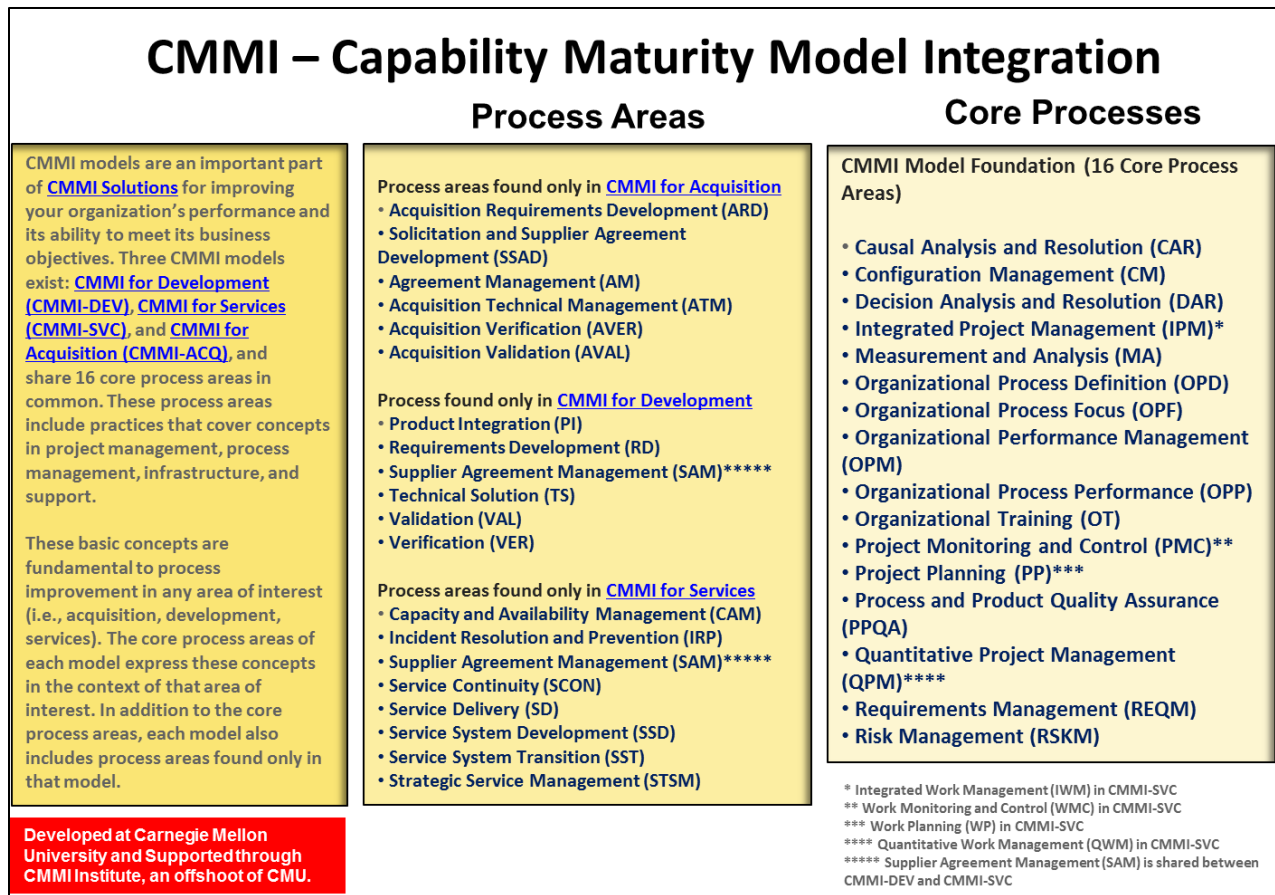


Figure 19: CMMI - Capability Maturity Model Integration

Developed by Carnegie Mellon University and available throughout the Information Technology arena, CMMI will provide a pathway to follow that will lead to maximum optimization of enterprise products, services, and operation.



## GRC – Governance, Regulations, and Compliance (Adhering to Laws and Regulations)

## Adhering to Compliance Laws

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **Dodd – Frank** – Wall Street Reform and Consumer Protection Act;
- **HIPAA** – Healthcare regulations (including ePHI, HITECH, and Final Ombudsman Rule);
- **Sarbanes – Oxley Act** (sections 302, 404, and 409) on financial assessment and reporting by authorized “Signing Officer”;
- **EPA and Superfund** (how it applies to Dumping and Asset Management Disposal);
- **Supply Chain Management** “Laws and Guidelines” included in **ISO 24762** (SSAE 16 for Domestic compliance and SSAE 3402 for International Compliance, and NIST 800-34);
- **Supply Chain Management** “Technical Guidelines” described in **ISO 27031**;
- **Patriots Act** (Know Your Customer, Money Laundering, etc.);
- **Workplace Safety and Violence Prevention** via OSHA, OEM, DHS, and governmental regulations (State Workplace Guidelines and Building Requirements);
- **Income Tax and Financial Information protection** via **Office of the Comptroller of the Currency** (OCC) regulations (**Foreign Corrupt Practices Act**, **OCC-177** Contingency Recovery Plan, **OCC-187** Identifying Financial Records, **OCC-229** Access Controls, and **OCC-226** End User Computing).



Figure 20: GRC (Governance, Regulations, and Compliance) Adherence

GRC and Compliance have been required for years and organizations have spent tremendous amounts of money adhering to these requirements. It still goes on, but now with new leadership in Washington, DC, laws and regulations may change, and compliance may have to be re-achieved.

Supply Chain Management (Managing Supplies and their Delivery Locations)

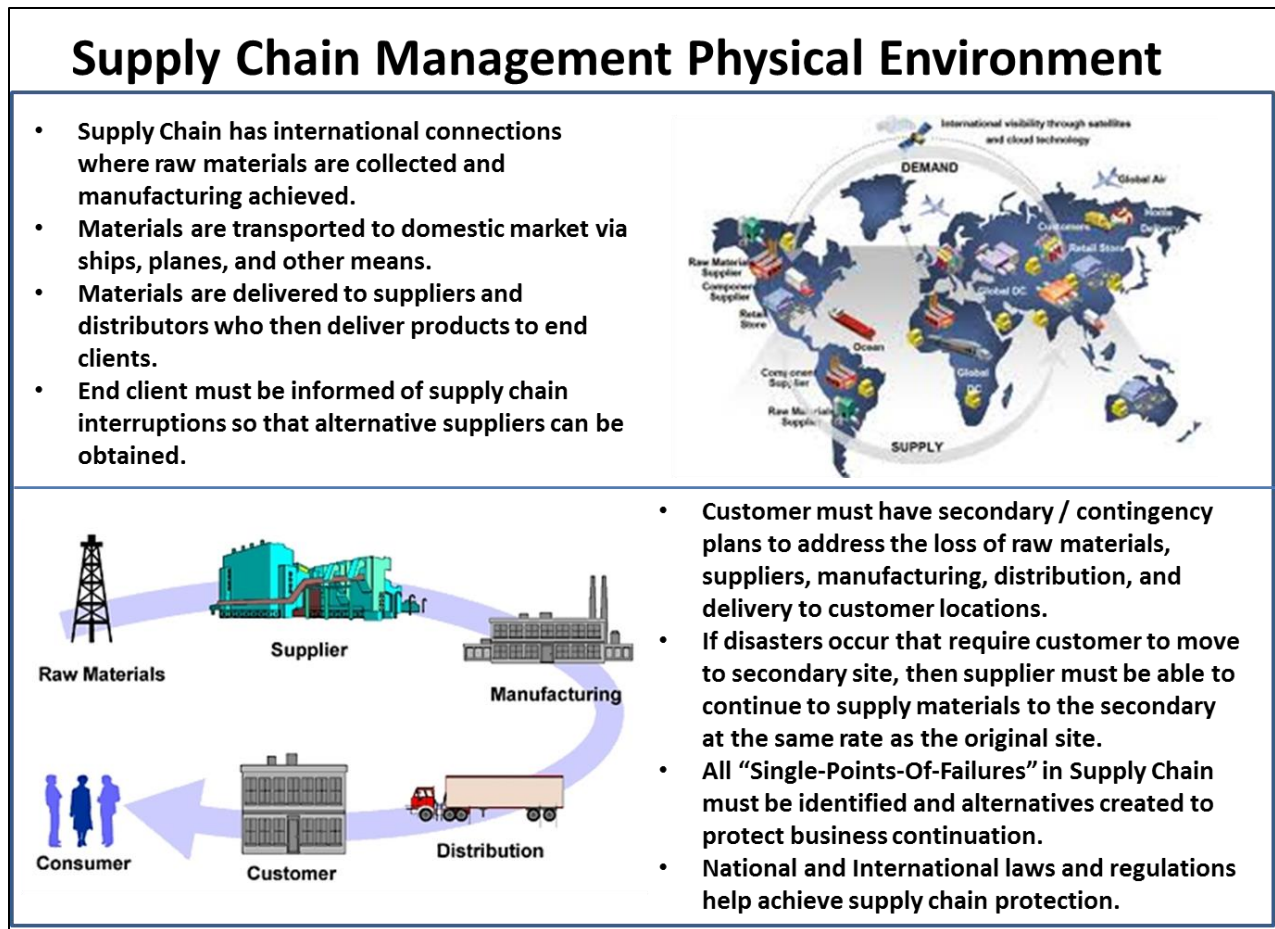


Figure 21: Supply Chain Management

Managing supplies needed to run a company is every executive’s concern. Supply Chain Management involves obtaining raw materials, shipping the raw materials to a plant or foundry for conversion to a product. Then the product must be distributed and sold. Interruption could result in loss business and fines built within contracts, so it is critical to optimize your Supply Chain Management process.

Systems Management and Controls – Workflow

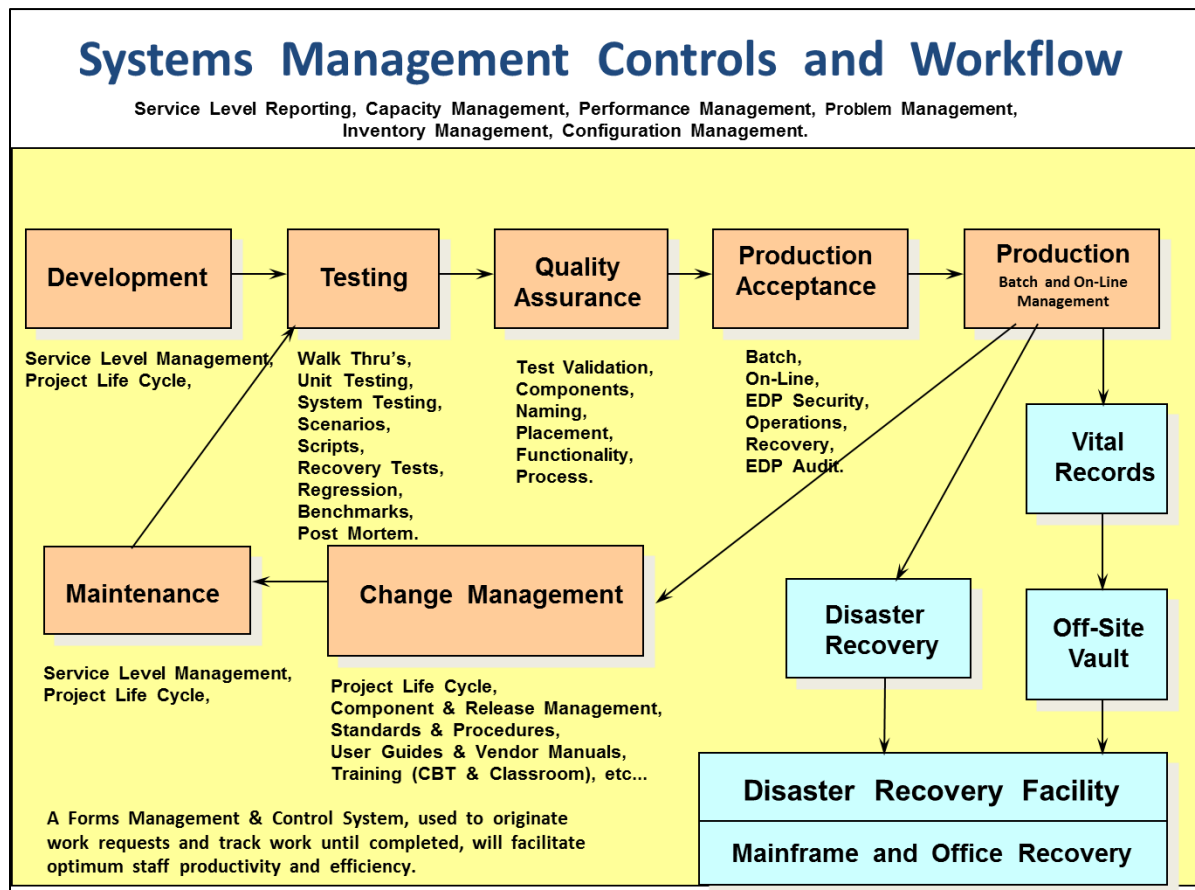


Figure 22: Systems Management Disciplines described.

Systems Management provides the needed Information Technology services described above.

Systems Management Organizational Structure

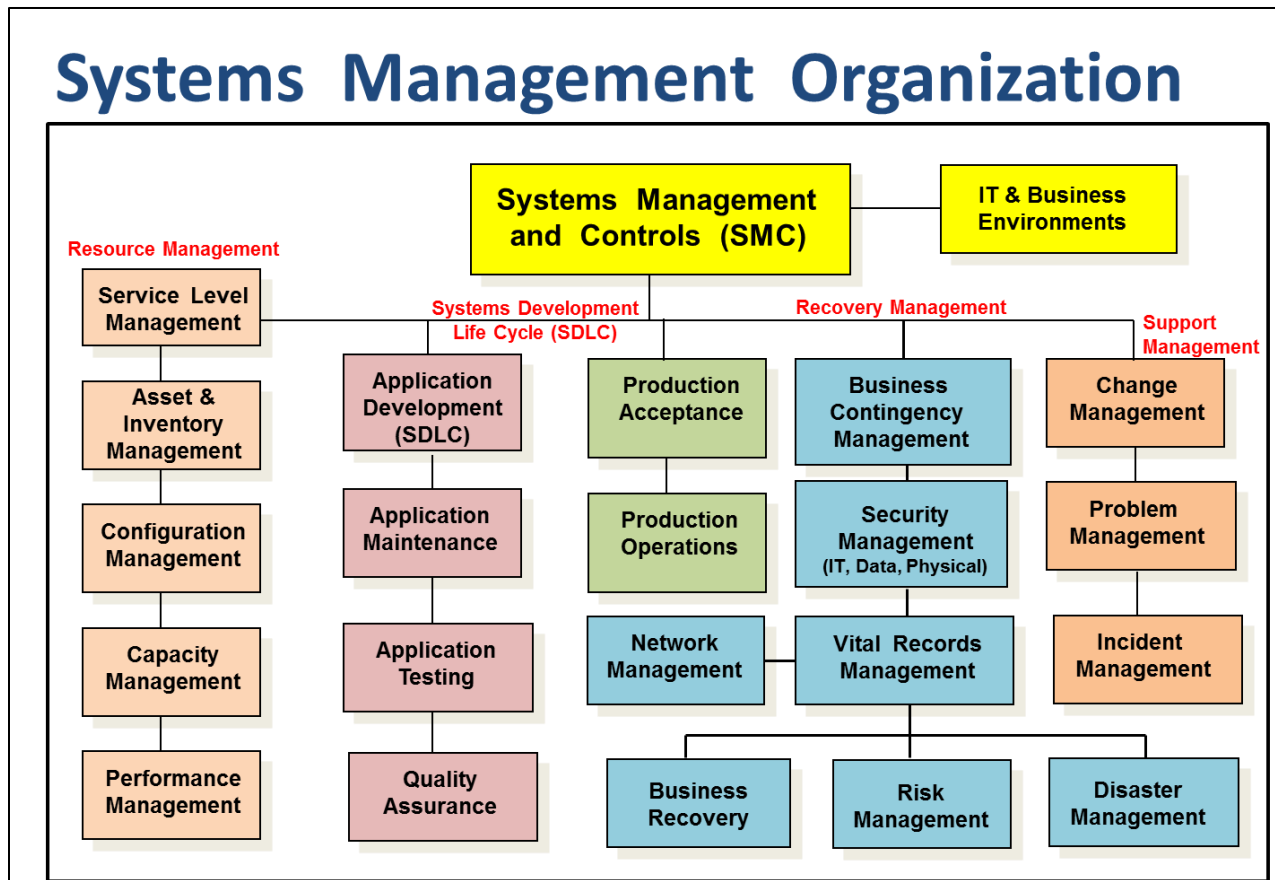


Figure 23: Systems Management Organizational Structure

The Systems Management Organizational Structure divides disciplines into categories managed by an enterprise.

SDLC – Systems Development Life Cycle (Migrating Applications to Production)

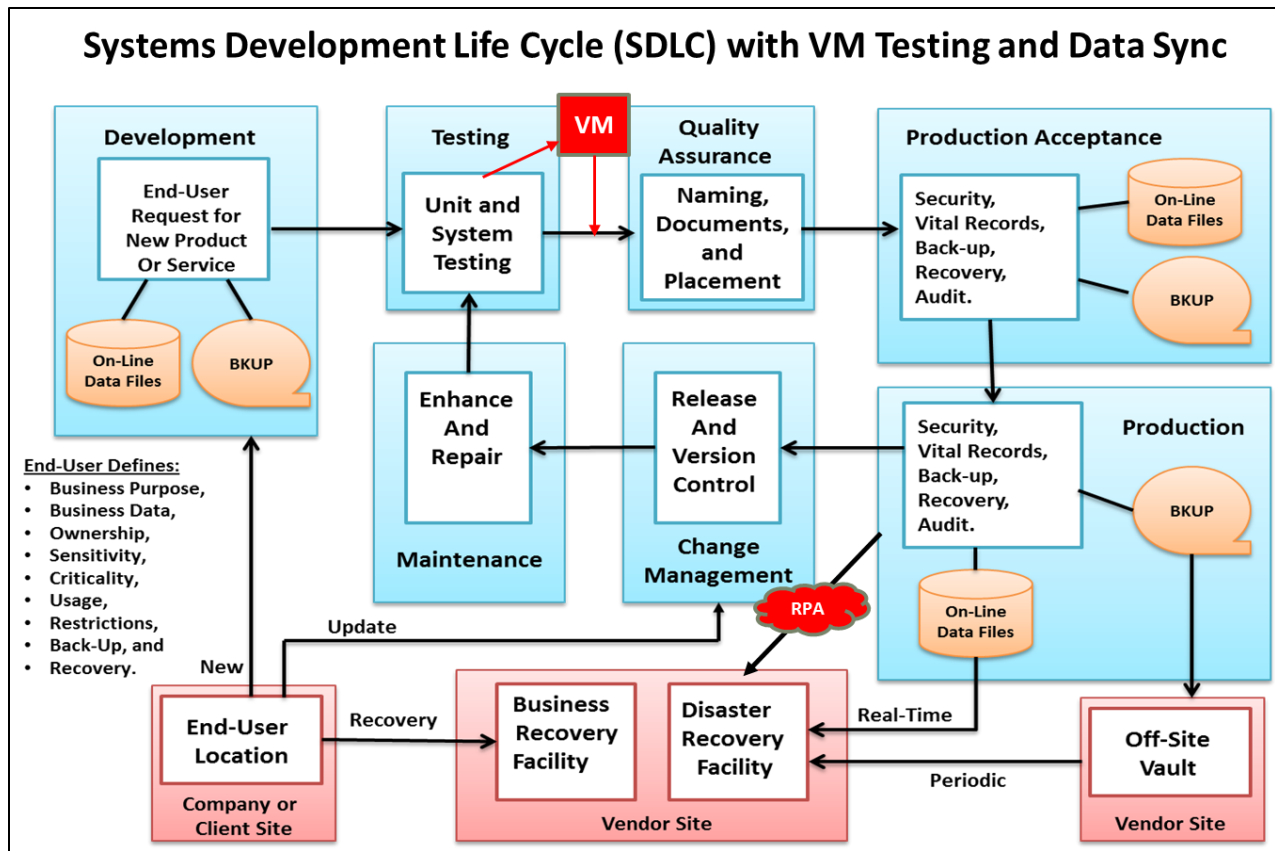


Figure 24: Systems Development Life Cycle

The Systems Development Life Cycle (SDLC) migrates applications, products, and services to Production in the manner shown above.

I hope this article helped you understand more about security management and how it is evolving in today's environment. Any comments or recommendations for improvement are gladly accepted.

If you would like to discuss the information contained in this document, or believe my services could be helpful to your organization, I can be contact at [bronackt@gmail.com](mailto:bronackt@gmail.com)

Thank you,

Tom Bronack