

Products...As-Is...Business Line...Information Technology

Table of contents

- 1 Information Technology..... 3
 - 1.1 Cyber Security Process.....7
 - 1.1.1 Establish Policies & Procedures..... 10
 - 1.1.2 Conduct Training and Awareness..... 11
 - 1.1.3 Protect the Boundary of the VA Infrastructure..... 11
 - 1.1.4 Certification and Accreditation..... 13
 - 1.1.5 Identification, Authentication, and Authorization..... 14
 - 1.1.6 Monitor, Report, & Respond..... 15
 - 1.2 Network Communication / Telecommunications Process..... 17
 - 1.2.1 Planning and Engineering..... 19
 - 1.2.2 Configuration Management..... 20
 - 1.2.3 Emergency Preparedness..... 22
 - 1.2.4 Operations and Security..... 22
 - 1.2.5 Order Handling..... 24
 - 1.2.6 Service Implementation..... 24
 - 1.2.7 Customer Service..... 26
 - 1.2.8 Quality Management.....27
 - 1.3 Data Center with Continuity of Operations (COOP) Process..... 28
 - 1.3.1 Acquire Customers.....29
 - 1.3.2 Deliver Services..... 31
 - 1.3.3 Assess Risk..... 32
 - 1.3.4 Mitigate Risk..... 33

1.3.5 Test Plans.....	34
1.3.6 Event Management.....	35
1.3.7 Maintaining Plans.....	36
1.4 Enterprise Architecture Process.....	37

1. Information Technology

The major functions within this business line are the four items denoted surrounding "Information Systems Management Organizations" (the organization responsible for carrying out these actions): Data Center with Contuinuity of Operations, Enterprise Architecture, Cyber Security, and Network Communications/Telecommunications. This diagram shows the major stakeholders and some of the relationships between those stakeholders, the agency, and its denoted functions.

Scroll down for descriptions of objects shown in this diagram. Clicking over a function name can directly bring up related process diagrams and activity descriptions.

Links to Z11 (listed alphabetically)	
Name	Description
Acquisition and Materiel Management Services	Various logistics support services for the benefit of internal VA organizations. These include procurement, inventory management and delivery.
Administrative Services	Enterprise administrative service resources provided by organizations internal to VA.
Agency Funding Requests	Budget proposals and other forms of requests for funding that VA sends to Congress and other funding approval bodies.
Agency Reports	Standard and ad-hoc reports about VA operations that are prepared and submitted to external organizations and oversight groups.
Agreements and Contracts	Formal agreements and contracts with parties outside VA .
Contracted Services	Enterprise contractual service resources provided by organizations external to VA.
Financial Services	Enterprise accounting and finance service resources provided by organizations internal to VA.

Human Resources	VA personnel including employees and contractors.
Internal Information Technology Services	Enterprise information-technology service resources provided by organizations internal to VA.
Official Government Guidance	Government circulars and other official guidance from external organizations that affect VA's operations.
Personnel Services	Enterprise personnel service resources provided by organizations internal to VA.
Physical Products	Product resources from external origins that are physical in nature.
Requests for VA Actions	Information contained in requests for VA action coming from sources external to VA .
Training Services	Training and other skills development services available to veterans and other program beneficiaries, service partners, and other entities outside the VA organization.
VA Program Funds	Monetary resource products from external sources for use in funding VA programs.
Vendor Services	Enterprise vendor service resources provided by organizations external to VA.

Links to Z12 (listed alphabetically)	
Name	Description
Cyber Security	The mission of Cyber Security, taken from the Information Technology Strategic Plan April 2002, DRAFT, is to secure the VA enterprise against cyber attack
Data Center with Continuity of Operations (COOP)	Data Center Operations with Continuity of Operations (COOP) is a sub-function of Information Technology (IT) and begins with a series of steps involving requirements definition, risk assessment,

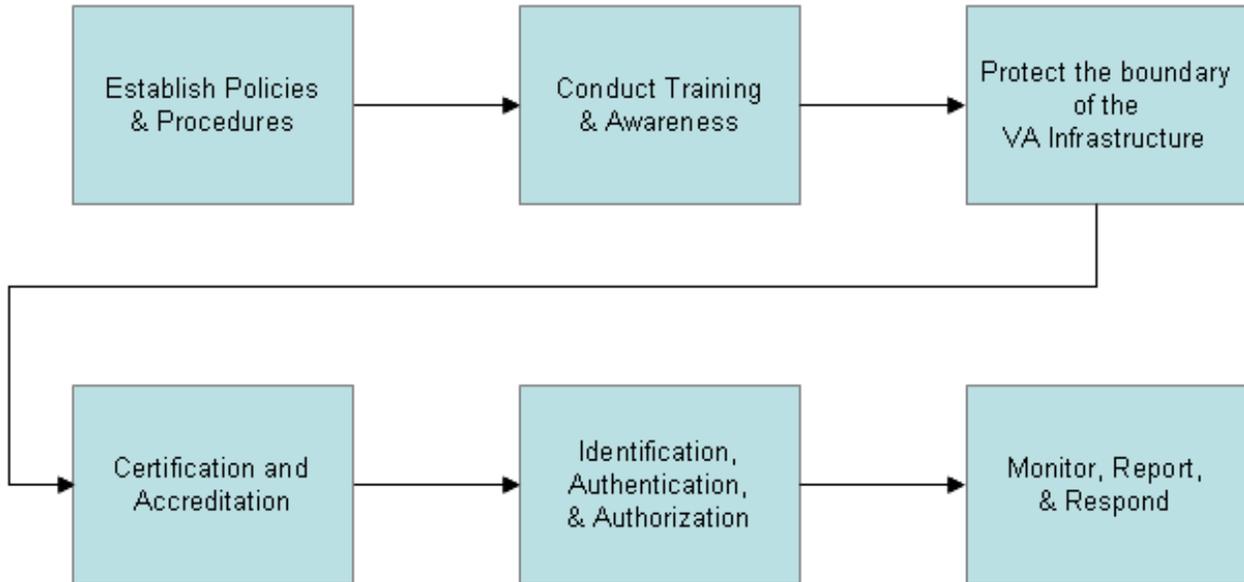
	<p>business impact analysis, and emergency preparedness/risk mitigation. Once the customers requirements are understood and documented, service delivery can begin. Once day-to-day processes are in place, the COOP focus turns to crisis management and business resumption planning.</p>
<p>Enterprise Architecture</p>	<p>Enterprise Architecture is fundamental for enabling an enterprise to assimilate internal changes in response to the external dynamics and uncertainties of the information age environment. It not only constitutes a baseline for managing change, but also provides the mechanism by which the reality of the enterprise and its systems can be aligned with management intentions. (John A. Zachman, President, Zachman International)</p> <p>The Department of Veterans Affairs (VA) Enterprise Architecture strategy was developed and unanimously approved by the VA Enterprise Architecture Innovation Team and signed by the Secretary in September of 2001. Enterprise Architecture is a continuous improvement process. The One-VA EA Program Management Plan (PMP) defines the processes and approach that allow for the integration of Enterprise Architecture processes, Capital Planning and Budgeting processes, and Project Management Oversight processes of the VA.</p> <p>The VA's EA mission is to develop and implement an evolutionary, high-performance, One-VA information technology architecture, aligned with our program and business goals that enable enterprise-wide function, process, and data integration.</p>
<p>Network Communication / Telecommunications</p>	<p>Network Communications/Telecommunications is responsible for the creation and administration of policies, standards, and guidelines to support the implementation, operation, and maintenance of networking and communication services and equipment for VA.</p>

Links to Z14 (listed alphabetically)	
Name	Description
Contractors	Individuals or organizations outside of VA that work for the Department under any of the various types of contractual arrangements or fee structures.
Government Policy Makers (Owners)	A category of VA stakeholders. Stakeholders falling under this category possess the authority to create and enforce major government policies and regulations that affect the Department of Veterans Affairs.
Managers	VA employees who plan, lead, organize, and control the operations of a well-defined VA organizational unit.
Workers	Non-managerial VA personnel.

Links to Z22 (listed alphabetically)	
Name	Description
Cyber Security Process	The mission of Cyber Security, taken from the Information Technology Strategic Plan April 2002, DRAFT, is to secure the VA enterprise against cyber attack
Data Center with Continuity of Operations (COOP) Process	Data Center Operations with Continuity of Operations (COOP) is a sub-function of Information Technology (IT) and begins with a series of steps involving requirements definition, risk assessment, business impact analysis, and emergency preparedness/risk mitigation. Once the customers requirements are understood and documented, service delivery can begin. Once day-to-day processes are in place, the COOP focus turns to crisis management and business resumption planning.
Enterprise Architecture Process	Enterprise Architecture is fundamental for enabling

	<p>an enterprise to assimilate internal changes in response to the external dynamics and uncertainties of the information age environment. It not only constitutes a baseline for managing change, but also provides the mechanism by which the reality of the enterprise and its systems can be aligned with management intentions. (John A. Zachman, President, Zachman International)</p> <p>The Department of Veterans Affairs (VA) Enterprise Architecture strategy was developed and unanimously approved by the VA Enterprise Architecture Innovation Team and signed by the Secretary in September of 2001. Enterprise Architecture is a continuous improvement process. The One-VA EA Program Management Plan (PMP) defines the processes and approach that allow for the integration of Enterprise Architecture processes, Capital Planning and Budgeting processes, and Project Management Oversight processes of the VA.</p> <p>The VA's EA mission is to develop and implement an evolutionary, high-performance, One-VA information technology architecture, aligned with our program and business goals that enable enterprise-wide function, process, and data integration.</p>
<p>Network Communication / Telecommunications Process</p>	<p>Network Communications/Telecommunications is responsible for the creation and administration of policies, standards, and guidelines to support the implementation, operation, and maintenance of networking and communication services and equipment for VA.</p>

1.1. Cyber Security Process



Reference(s):

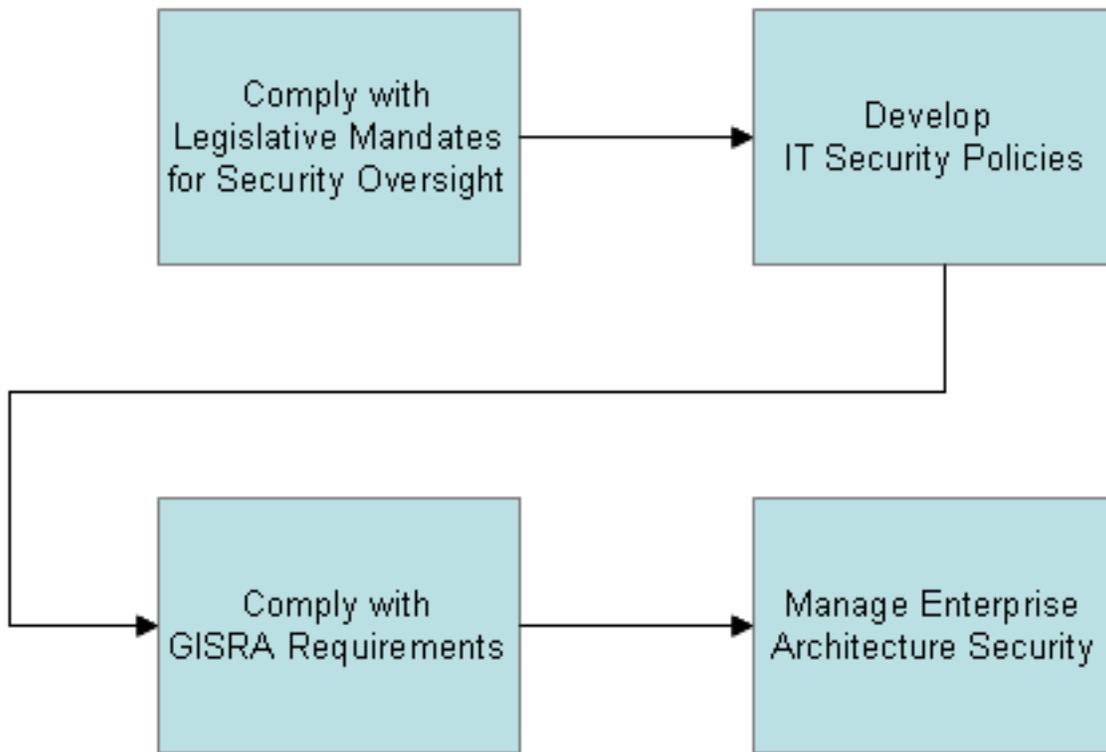
- IT Cyber Security.html

Links to Z22 (listed alphabetically)	
Name	Description
Certification and Accreditation	The function deals with the certification and accreditation of the application and systems implement within the VA infrastructure. Beyond the initial certification and accreditation is a set of activities that monitor the continued performance of the individual, application, or system to ensure that it maintains the defined security posture.
Conduct Training & Awareness	This -function includes all activities dealing with the education of the workforce on cyber security topics, VA policies, governing laws and regulations, recommended and approved procedures, potential threats and countermeasure, and individual response to incidences and certification of the security profession stating their level of achievement. For the average VA employee who uses electronic systems to conduct their tasks this function is responsible for

	<p>maintaining their awareness to cyber security. For the Security staff member, the function establishes technical and management training programs for career development and enhancement of job knowledge and certification of achievement.</p>
<p>Establish Policies & Procedures</p>	<p>This function has many activities that include: (1) understanding the legal requirements placed on the VA to protect the confidentiality and integrity of an individual's data; (2) establishing the policies and procedures that ensure the governing requirements are met; (3) reporting to the governing and oversight bodies the adherence to the requirements; and (4) collecting, analyzing and recommending security practices that have been accepted in the industry.</p>
<p>Identification, Authentication, & Authorization</p>	<p>This sub-function deals with several IT responsibilities, including: (1) the establishment of the positive identification of an individual or system; (2) defining, distributing, and managing the identification credentials; (3) verifying that the individual is who they say they are; (4) validating the authenticity of the presented identification credentials; (5) compiling and maintain access permissions by data element/classes or by devices/locations/systems/networks; (6) defining and implementing access controls for application, data stores, systems, and networks; (7) verifying that a request for access is allowable; (8) monitoring and reporting violations of access controls; (9) maintaining an auditable record for data access and processing and, where appropriate, with ensuring architecture components are certified to appropriate levels of government certification; and (10) enhancing secure interoperability with other government organizations.</p>
<p>Monitor, Report, & Respond</p>	<p>This function monitors the infrastructure for violations of security policy or procedures, unauthorized attempts for access, cyber attacks, events, and trends in the external world, and denial of service. Each monitored incident is documented, investigated, and reported. Activities that define the VA response to events are demanded. All response activities are designed to prevent unauthorized access and maintain data integrity throughout the enterprise.</p>

<p>Protect the Boundary of the VA Infrastructure</p>	<p>This function applies security technology and policies to the interfaces among the VA Infrastructure components and between the VA Infrastructure and the external world. These include establishing protection & searching for malicious code, unauthorized access, intrusion detection, denial of service. There are seven (7) layers of defense as defined by the VA CIO to be implement and managed under this function.</p>
--	---

1.1.1. Establish Policies & Procedures



Links to Z22 (listed alphabetically)	
Name	Description
Comply with GISRA Requirements	Maintenance and support of the Government Information Security Reform Act (GISRA) database

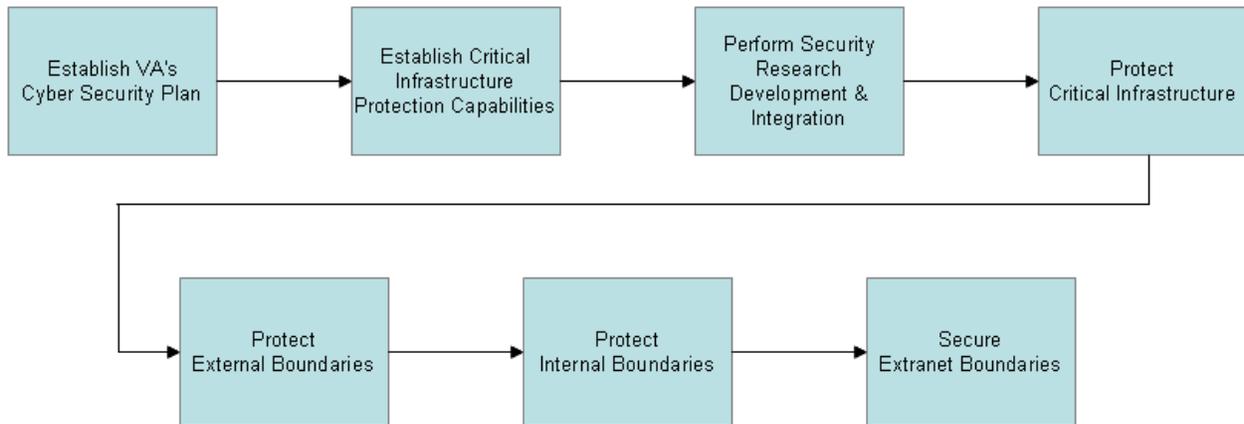
	and preparation of the annual and quarterly reports.
Comply with Legislative Mandates for Security Oversight	Establish procedures to evaluate VA Infrastructure for compliance with laws and directives.
Develop IT Security Policies	Manage security-specific policies and guidance.
Manage Enterprise Architecture Security	Implement security into the One-VA enterprise architecture.

1.1.2. Conduct Training and Awareness



Links to Z22 (listed alphabetically)	
Name	Description
Conduct Cyber Security Conferences	Design cyber security conferences and provide all logistical support for these conferences.
Conduct VA-wide Cyber Security Training	Provide Security Certification Training for Field Information Security Officers. Provide Security Training for all IT personnel. Provide Security Awareness Training for all personnel
Manage ISO Certifications	Maintain the ISO Certification process and its supporting resources. Support the Cyber Security Policy-making activity.

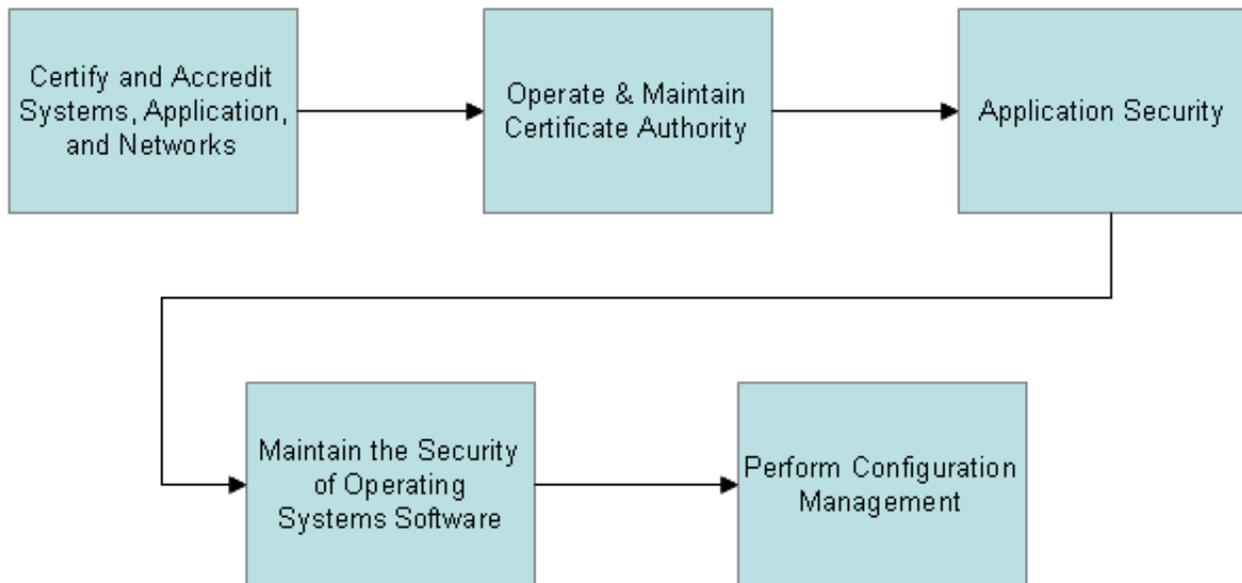
1.1.3. Protect the Boundary of the VA Infrastructure



Links to Z22 (listed alphabetically)	
Name	Description
Establish Critical Infrastructure Protection Capabilities	Secure the VA network boundaries with world-class technology. Reduce from over 200 independent gateways to 4 enterprise gateways that employ the “Defense-in-depth” strategy to protect VA from cyber attack. Establish a securable number of entry and exit points to the VA network.
Establish VA's Cyber Security Plan	This function performs the activities to develop a plan or course of action intended to influence and determine decisions, actions, and other matters concerning the maintenance of VA's electronic environment.
Perform Security Research Development & Integration	Perform research and testing of next generation information-security technology to ensure the Department maintains the highest level of effective protection by the most state of the art technology available.
Protect Critical Infrastructure	Protect information assets that are essential to continuous operations of the VA business lines. Effectively securing these information assets is critical to the Department's ability to safeguard its IT assets, maintain the confidentiality of sensitive veterans' health and disability benefits information, and ensure the reliability of its financial data. Harden

	critical devices.
Protect External Boundaries	Secure the interface between the VA Infrastructure and the external world.
Protect Internal Boundaries	Secure the interfaces among the internal VA Infrastructure components to limit adverse affects caused by an internal attack of event.
Secure Extranet Boundaries	Secure the interfaces among the internal VA Infrastructure and trusted external business associates.

1.1.4. Certification and Accreditation



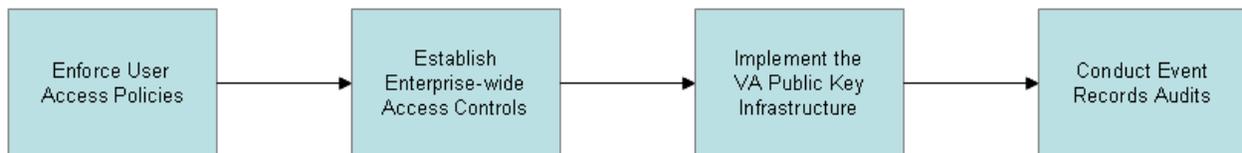
Reference(s):

- IT Cyber Security Security Certification and Accreditation.html

Links to Z22 (listed alphabetically)	
Name	Description

Application Security	Establish security profiles of applicants. Recommend appropriate security techniques and technologies to achieve the security profile. Maintain current understanding of security techniques and technologies, and maintain how they can be applied to achieve security objectives.
Certify and Accredite Systems, Application, and Networks	Establishes the Certification & Accreditation (C&A) procedures. Evaluates the system/application/network for certification. Recommends system/application/ network for accreditation.
Maintain the Security of Operating Systems Software	Establish the OS security profile. Identifies OS vulnerabilities. Maintains library of recommended OS patches and configuration. Inspects system for proper maintenance of OS security profiles.
Operate & Maintain Certificate Authority	Manages the Certificate Authority process.
Perform Configuration Management	Establish the system and network configurations to achieve a specified security profile. Inspect system or network devices for specified configuration. Monitor unauthorized changes to system or network configurations.

1.1.5. Identification, Authentication, and Authorization



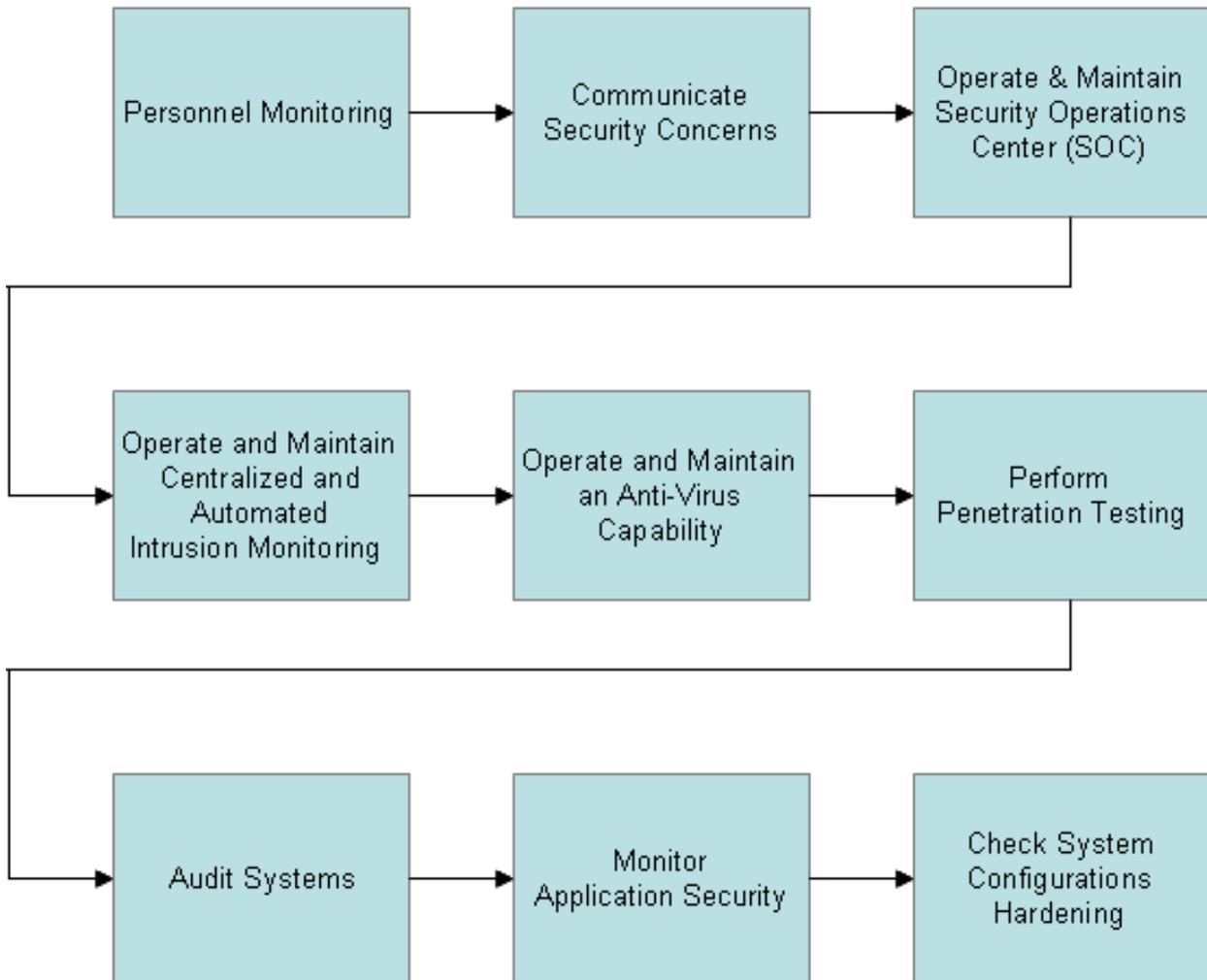
Reference(s):

- IT Cyber Security Authorization.html

Links to Z22 (listed alphabetically)	
Name	Description
Conduct Event Records Audits	Audit all access logs for evidence of attempted and

	actual unauthorized access to applications, systems, communications, networks, and data.
Enforce User Access Policies	Establish User Registration Procedures. Establish User Identification Procedures. Establish User Authentication Procedures. Establish User Authorization Procedures. Permit/Deny Access using a "least privilege" based permissions strategy. Establish Access Controls to Enforce Segregation of Duties. Log access events.
Establish Enterprise-wide Access Controls	Establish the framework under which applications will use enterprise wide access controls.
Implement the VA Public Key Infrastructure	Establish the framework and perform pilot programs to oversee and facilitate implementation of PKI Department wide.

1.1.6. Monitor, Report, & Respond



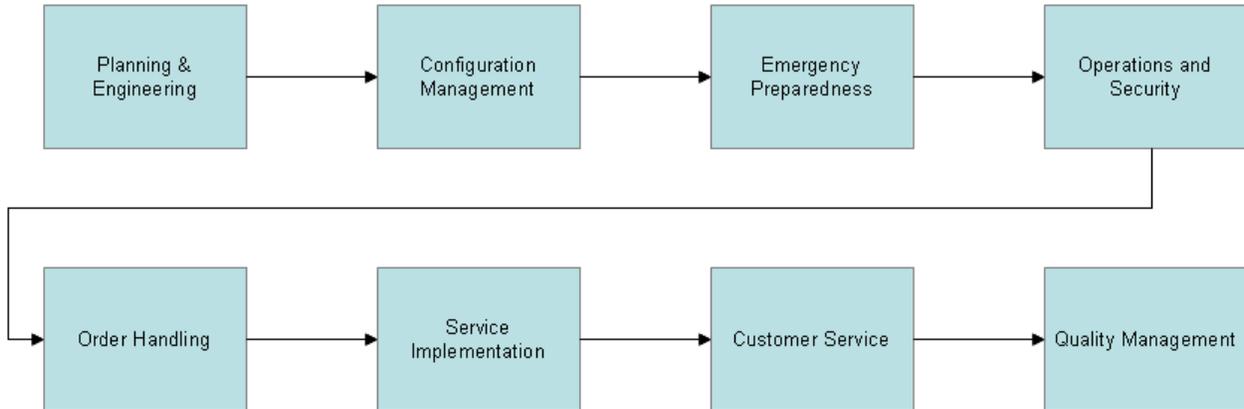
Reference(s):

- [IT Cyber Security Monitoring.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Audit Systems	Use periodic, routine auditing to monitor for security profile maintenance and evidence of authorized activity. Establish procedures for separation of duties.

Check System Configurations Hardening	Monitor system, application, network, and data stores for proper hardening configurations.
Communicate Security Concerns	Operate, & maintain an IT Command, Control & Communication (C3) infrastructure
Monitor Application Security	Monitor application performance for evidence of security breaches.
Operate & Maintain an Anti-Virus Capability	Select, install, and maintain anti-virus capability VA-wide.C28
Operate & Maintain Centralized & Automated Intrusion Monitoring	Establish and upgrade the VA-CIRC using “best-of-class” managed cyber security services from private industry. Manage and monitor the VA network using the VA-CIRC and SOC’s as supporting entities to mitigate, respond, and remedy cyber security threats.
Operate & Maintain Security Operations Center (SOC)	Equip, manage, and staff two Security Operations Centers (SOC’s) to monitor the security devices installed at the CDPC’s and RDPC’s.
Perform Penetration Testing	Perform “Red Team” activities to test and “attack” the VA network boundary and intranet to identify and eliminate weaknesses before they can be exploited.
Personnel Monitoring	Control Personnel Activities through Formal Operating Procedures, Supervision, and Review

1.2. Network Communication / Telecommunications Process



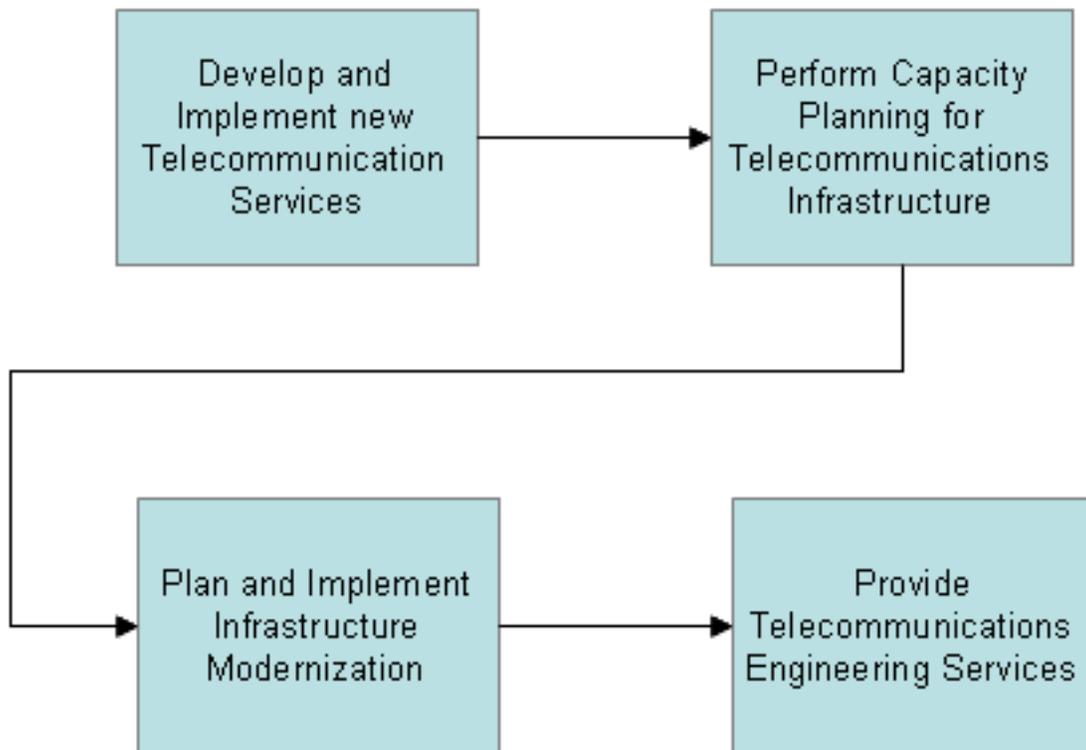
Reference(s):

- [IT Cyber Security Communication.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Configuration Management	This function includes activities associated with the resource management of the telecommunications infrastructure.
Customer Service	This function includes activities associated with the daily interaction and support of users of telecommunications services.
Emergency Preparedness	This function involves emergency planning activities associated with the Telecommunications support of the Continuity of Operations Plan (COOP) and the National Continuity of Government (COG) initiatives.
Operations and Security	This function includes activities associated with the daily management of the telecommunications networks and services.
Order Handling	This function includes activities associated with the creation and processing of service requests for telecommunication services.

Planning & Engineering	This function includes activities associated with the development, implementation, expansion, and modernization of the telecommunications infrastructure.
Quality Management	This sub-function includes activities associated with ensuring the quality and performance of telecommunication services.
Service Implementation	This function includes activities associated with the implementation of telecommunication services.

1.2.1. Planning and Engineering



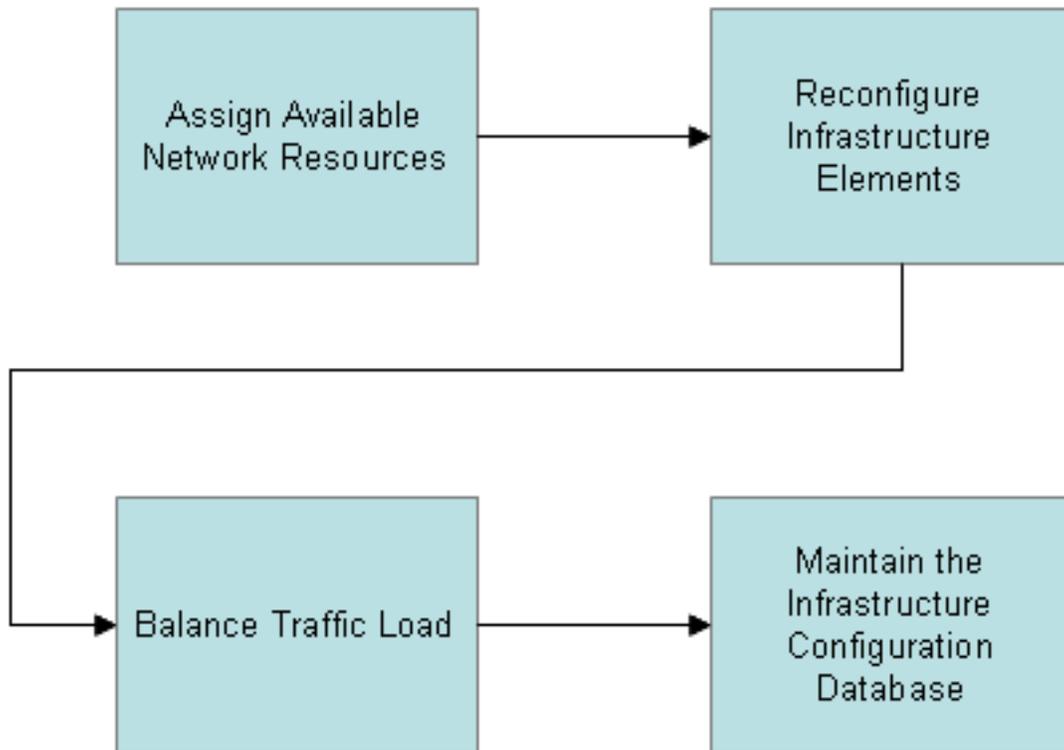
Reference(s):

- IT Cyber Security Communication Planning.html

Links to Z22 (listed alphabetically)

Name	Description
Develop and Implement new Telecommunication Services	Identify new technologies that can be incorporated in the VA network architecture or in customers' telecommunications systems. Recommend improvements in VA telecommunication networks. Price and offer new services to potential customers.
Perform Capacity Planning for Telecommunications Infrastructure	Forecast the volume of telecommunication traffic within VA. Assess the capability of the existing telecommunications infrastructure to handle current and future requirements.
Plan and Implement Infrastructure Modernization	Prepare designs for telecommunications infrastructure improvements or expansions. Acquire project funding and implement modernization plans.
Provide Telecommunications Engineering Services	Sell telecommunications engineering services to other organizations. Formalize service agreements. Deliver telecommunication products and services to other organizations.

1.2.2. Configuration Management



Reference(s):

- [IT Cyber Security Communication Configuration Management.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Assign Available Network Resources	Decide on which systems will be connected to each network.
Balance Traffic Load	Allocate and reallocate telecommunications traffic to maintain relative balance in network loads.
Maintain the Infrastructure Configuration Database	Record every change in the infrastructure configuration. Update the infrastructure database.
Reconfigure Infrastructure Elements	Evaluate alternative configurations to determine the

	optimum combination of infrastructure elements. Implement the reconfigurations.
--	--

1.2.3. Emergency Preparedness

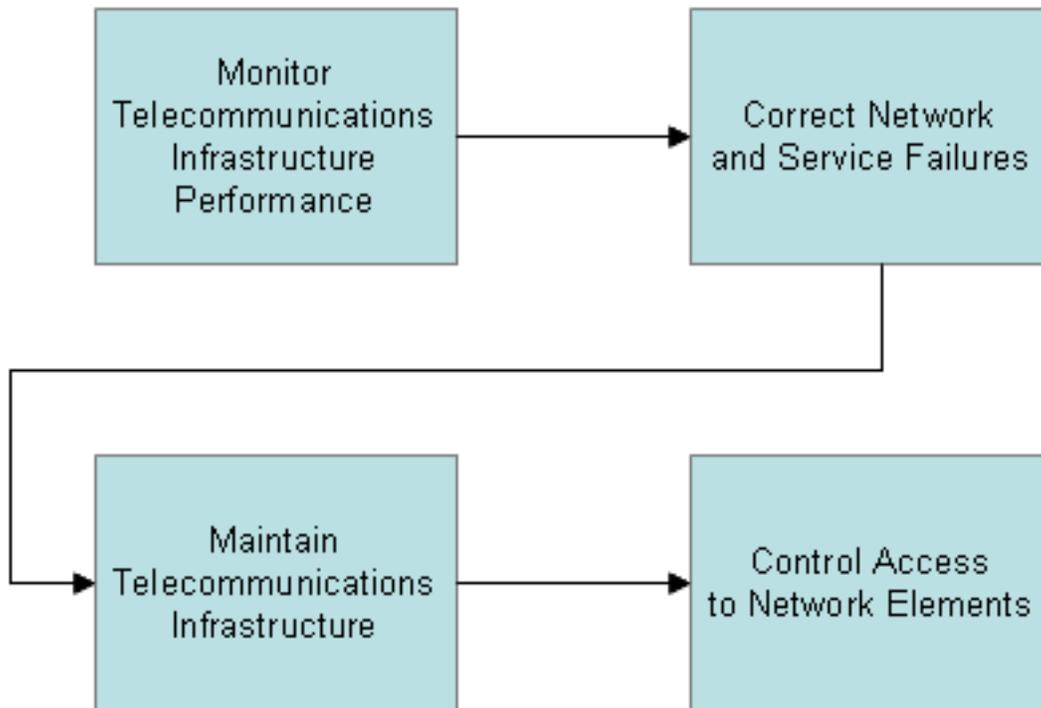


Reference(s):

- [IT Cyber Security Communication Emergency Preparedness.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Coordinate Emergency Issues with Other Agencies	Establish contingency plans that may involve sharing infrastructure resources with other agencies in case of emergencies.
Develop Emergency Plans	Decide on actions to be taken in case of an emergency. Develop emergency plans and procedures that identify the roles to be performed by certain individuals in the organization in the event of an emergency.
Develop Emergency Policies and Documentation	Prepare and disseminate formal guidelines for the installation and operation of communication networks during emergencies.

1.2.4. Operations and Security



Reference(s):

- [IT Cyber Security Communication Operation and Security.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Control Access to Network Elements	Control physical access to network elements. Manage the day-to-day security of network sites and act on access violations.
Correct Network and Service Failures	Analyze and solve technical problems encountered during network installation and operation activities. This includes analyses of network alert logs, outage records, element fault reports, and capacity and utilization reports.
Maintain Telecommunications Infrastructure	Perform routine preventive maintenance on the network infrastructure components.

Monitor Telecommunications Infrastructure Performance	Establish standards for the performance of telecommunications networks. Develop a methodology for data collection and analysis. Gather operating data and determine performance level relative to standards.
---	--

1.2.5. Order Handling

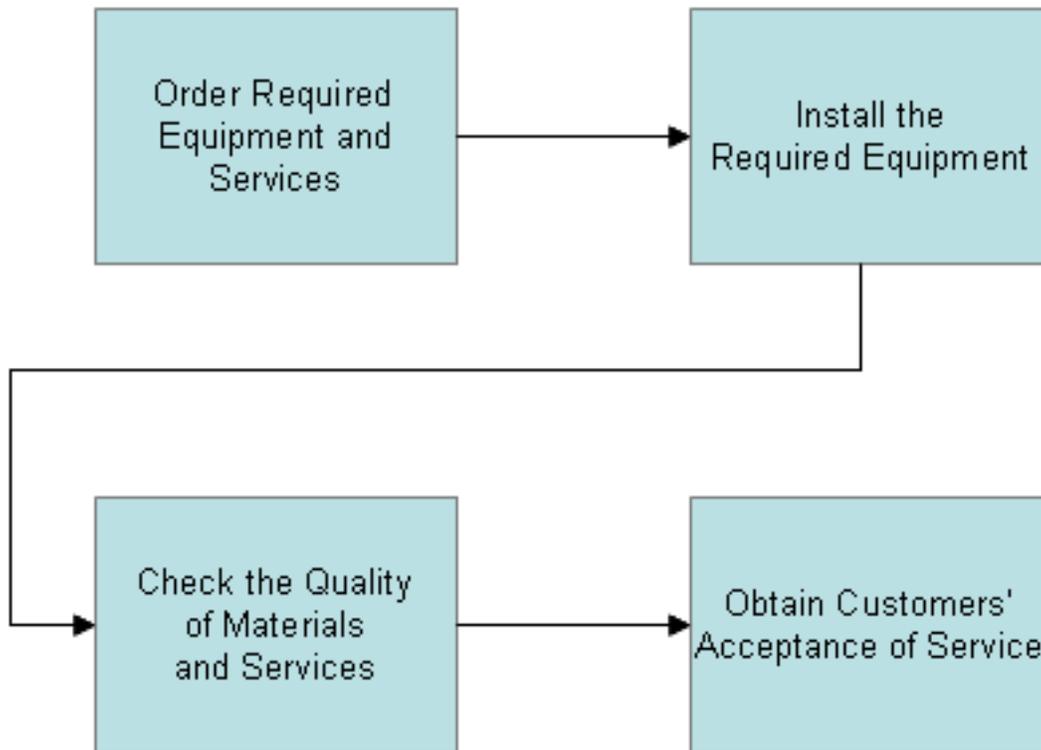


Reference(s):

- [IT Cyber Security Communication Order Handling.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Accept and Record Service Orders	Review incoming Service Orders. Enter Service Order information into the database once accepted.
Notify Customers of Completed Service Orders	Inform customers about completion of work under Service Orders.
Track Service Order Status	Track service order progress and provide status feedback to customers.

1.2.6. Service Implementation



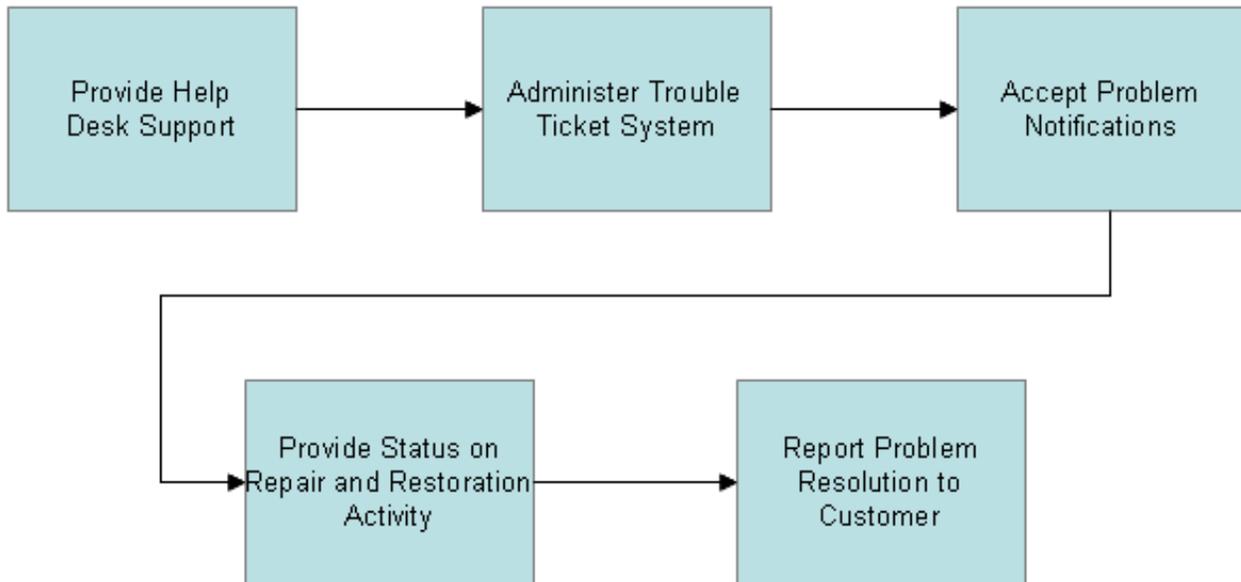
Reference(s):

- [IT Cyber Security Communication Service Implementation.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Check the Quality of Materials and Services	Determine the appropriate evaluation criteria for testing the installed telecommunication equipment and systems. Conduct tests on the installed systems.
Install the Required Equipment	Develop installation plans and schedules. Position materials and personnel. Implement installation plans.
Obtain Customers' Acceptance of Service	Make final adjustments or perform rework as needed. Get the customers to acknowledge formally

	work completion.
Order Required Equipment and Services	Determine required materials and services to complete each Service Order. Procure materials and services.

1.2.7. Customer Service



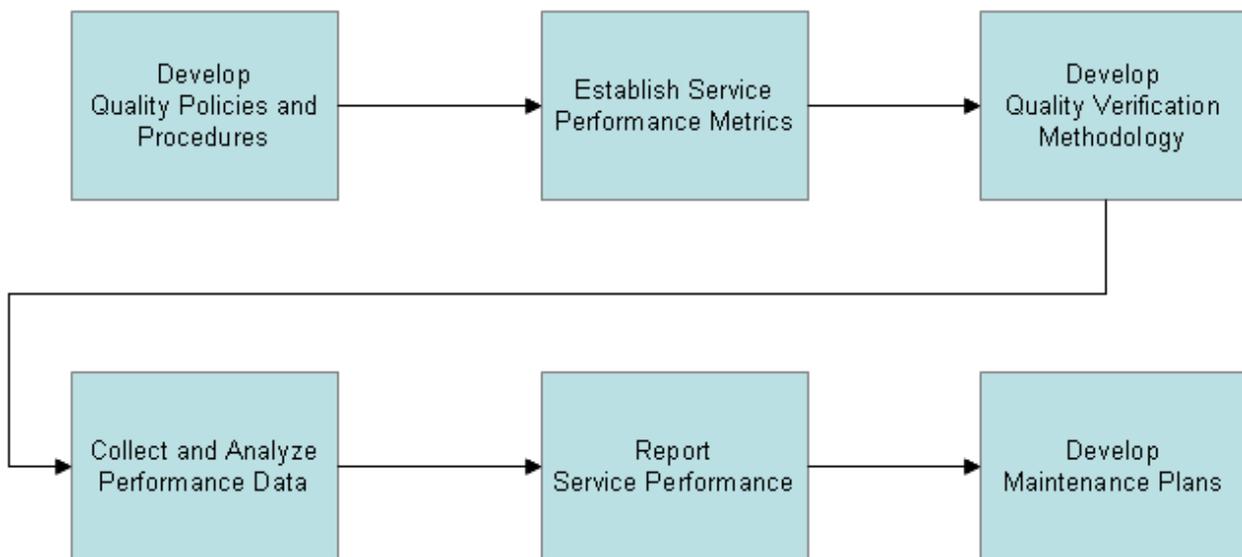
Reference(s):

- IT Cyber Security Communication Customer Service.html

Links to Z22 (listed alphabetically)	
Name	Description
Accept Problem Notifications	Receive formal requests for service as contained in Problem Notifications.
Administer Trouble Ticket System	Provide personnel and facilities to operate the Trouble Ticket System.

Provide Help Desk Support	Assist system users in solving day-to-day telecommunication infrastructure problems.
Provide Status on Repair and Restoration Activity	Provide customers with status information about repairs and restorations work.
Report Problem Resolution to Customer	Inform customers about actions taken on their Problem Notifications.

1.2.8. Quality Management



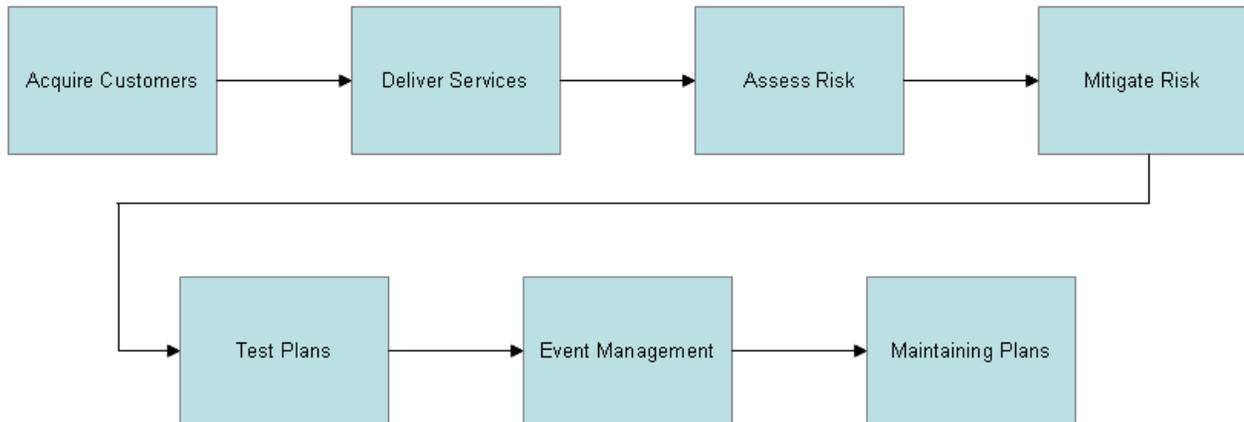
Reference(s):

- [IT Cyber Security Communication Quality Management.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Collect and Analyze Performance Data	Collect data items related to the performance metrics of networks. This includes data about bandwidth utilization, packet loss, throughput, network availability, etc. Compare actual performance with

	the standards that have been set.
Develop Maintenance Plans	Develop plans to maintain or improve the quality of network operations.
Develop Quality Policies and Procedures	Define basic operational policies and procedures. Set service performance objectives and define specific measures of performance.
Develop Quality Verification Methodology	Develop a detailed technical approach for the quality evaluation.
Establish Service Performance Metrics	Set service performance objectives and define specific measures of performance to be used. Decide on the metrics that will be utilized in the performance measurement.
Report Service Performance	Prepare and disseminate formal performance evaluation reports.

1.3. Data Center with Continuity of Operations (COOP) Process

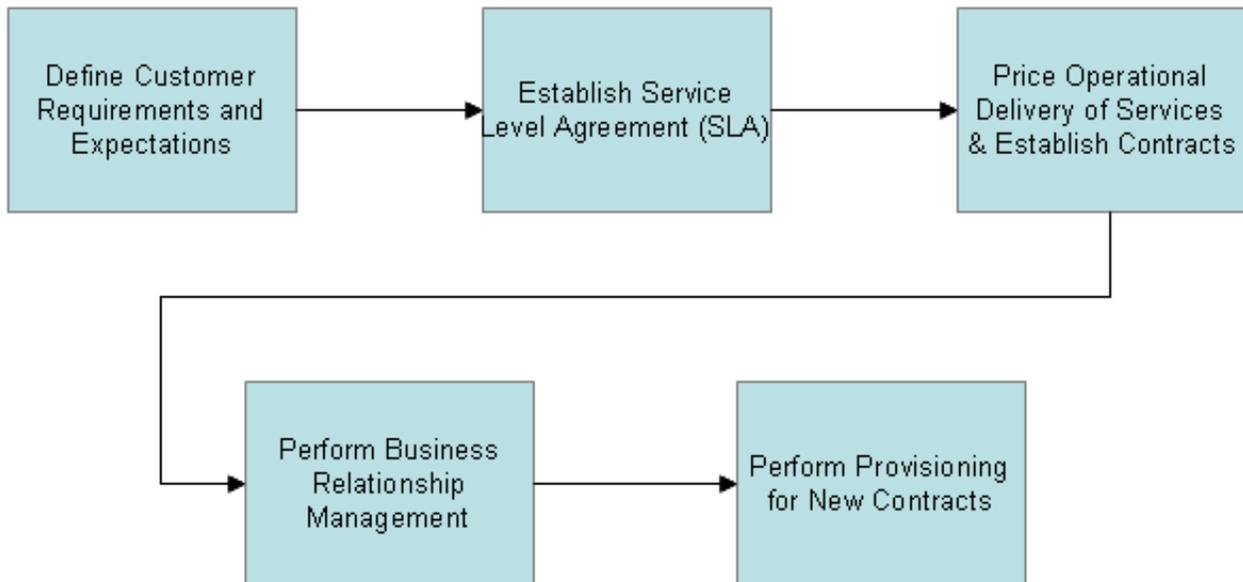


Reference(s):

- IT Cyber Security COOP.html

Links to Z22 (listed alphabetically)	
Name	Description
Acquire Customers	This function involves the activities associated with establishing a customer/provider relationship with the program owner to deliver services. It involves a systematic process for defining customer requirements and provider responsibilities for delivering a given level of service for a defined level of cost.
Assess Risk	This function assesses an organization's current risk posture and vulnerability, defining the probability of an event occurring that could interrupt services.
Deliver Services	This function involves the delivery of services on a periodic basis. Service delivery is based on predefined requirements and established recovery time and recovery point objectives based on the criticality of the system
Event Management	This function is responsible for identifying, documenting, and resolving incidents and events that influence the ability of the data center to deliver services
Maintaining Plans	This function is an on-going activity to update, improve, and modify the plans. It includes all the actions required to keep the plans up-to-date to be a useable product for the VA data center.
Mitigate Risk	This function encompasses the actions and activities to eliminate or reduce the degree of identified risk to the VA corporate data center.
Test Plans	This function develops the plan to ensure that data center COOP activities are tested according to a VA policy document.

1.3.1. Acquire Customers



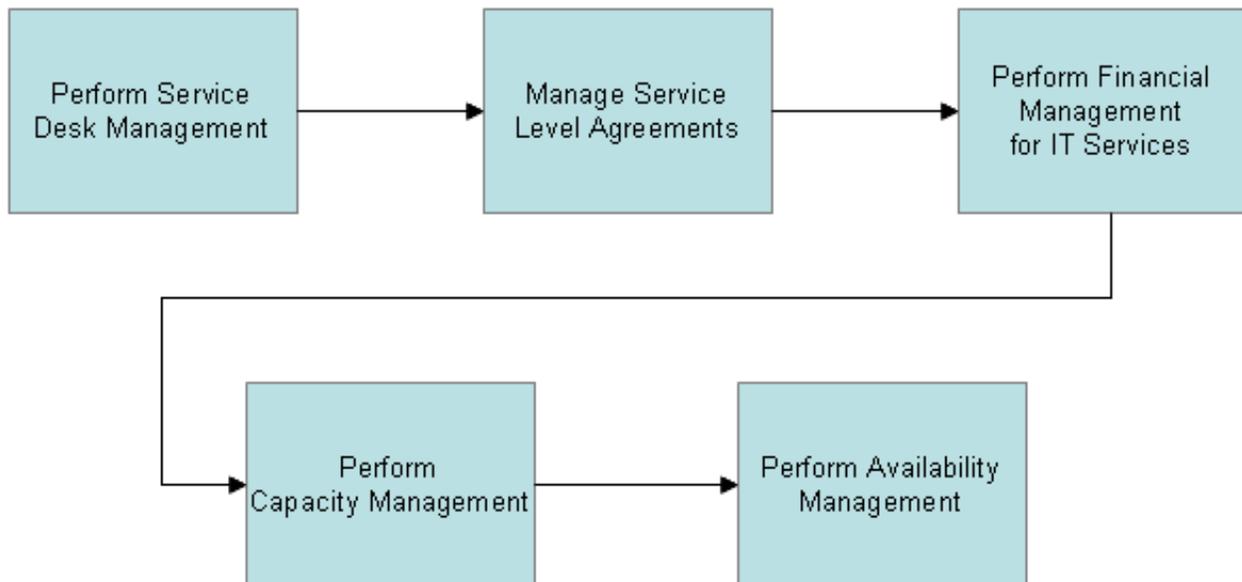
Reference(s):

- IT Cyber Security Communication COOP Acquire Customers.html

Links to Z22 (listed alphabetically)	
Name	Description
Define Customer Requirements and Expectations	A structured methodology for defining the basic operational requirements of a given system needed to perform a given business process. It is essentially a logical systems model.
Establish Service Level Agreement (SLA)	A systematic process of mapping logical requirements to an operational model defining those aspects of the service delivery that will be measured, the periodicity of the measures and the impact from non-performance. It is at this point that a system's RTO and RPO are defined.
Perform Business Relationship Management	This activity is associated with finalizing agreements, setting up necessary customer billing information, establishing key points of contact between the customer and provider prior to the actual delivery of

	services. This activity then continues with the customer over the life of the contractual relationship.
Perform Provisioning for New Contracts	This activity involves the process of acquiring the resources necessary to support the new contract/customer requirement. Involves activities associated with subcontract execution, provisioning from spare capacity held for this purpose, and modifying configuration management plans for technology.
Price Operational Delivery of Services & Establish Contracts	A systematic process of estimating the resources that will be consumed within the data center to support the PLSA. These estimates generally become the basis of an agreement between the customer and the provider for exchanging funds for services delivered.

1.3.2. Deliver Services



Reference(s):

- IT Cyber Security Communication COOP Deliver Services.html

Links to Z22 (listed alphabetically)	
Name	Description
Manage Service Level Agreements	This activity is responsible for ensuring that Service Level Agreements and contracts are met, and for ensuring that any adverse impacts on service quality are kept to a minimum.
Perform Availability Management	This activity is concerned with the design, implementation, measurements, and management of IT services to ensure consistently meeting the stated requirements for availability.
Perform Capacity Management	This activity is responsible for ensuring adequate capacity is available at all times to meet the requirements of the data center.
Perform Financial Management for IT Services	This activity is responsible for accounting for the costs (costing) and return on IT service investments, IT portfolio management and for cost recovery.
Perform Service Desk Management	Provides a single point of contact between the data center and its user customers. It is also the focal point for related service delivery and Event Management (Service Support) subfunctions.

1.3.3. Assess Risk



Reference(s):

- IT Cyber Security Communication COOP Assess Risk.html

Links to Z22 (listed alphabetically)	
Name	Description
Assess Business Impact of Non-availability	A management level analysis, which identifies the impacts of losing resources associated with EBFs and KEFs. The Business Impact of non-availability, measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning. The focus is on the IT systems and applications supporting these EBFs and KEFs.
Assess Risk that Could Cause Non-availability	A systematic process for identifying and categorizing risk vulnerabilities that may affect the mission of the entity. In this instance, it is the risk to the continued availability of data and processing that affects either the KEF or EBF.

1.3.4. Mitigate Risk



Reference(s):

- IT Cyber Security Communication COOP Mitigate Risk.html

Links to Z22 (listed alphabetically)	
Name	Description
Develop and Implement Risk Mitigation Strategies	Actions and activities to eliminate or reduce the degree of risk to life and property from hazards. As applied to data and applications, it is the steps taken to ensure that systems and data remain available to the various VA business functions.

Plan for Business Continuity	Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue without material interruption or essential change.
Plan for Disaster Recovery	Process of developing advance arrangements and procedures that enable an organization to respond to a disaster and resume the critical functions within a predetermined period, minimize the amount of loss, and repair or replace the damaged facilities as soon as possible.

1.3.5. Test Plans



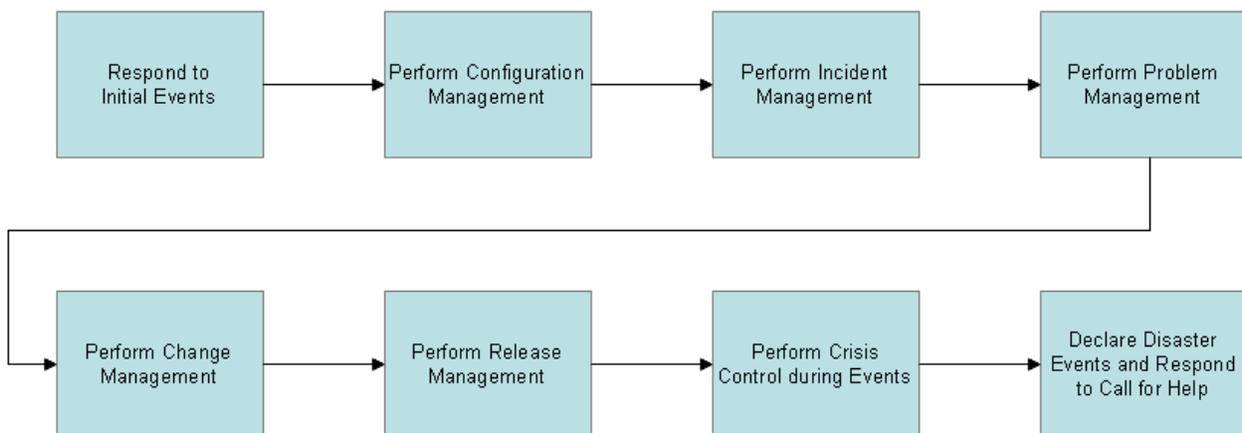
Reference(s):

- [IT Cyber Security Communication COOP Test Plans.html](#)

Links to Z22 (listed alphabetically)	
Name	Description
Test Business Continuity Plan	Tests are conducted as a schedule of announced and unannounced practice drills designed to identify and resolve weaknesses in the plan. Different scenarios are used to test different aspects of the plan. Drills can range from tabletop exercises to full dress rehearsals. Some elements of the risk mitigation strategies can be tested routinely without affecting operations, (e.g. generator tests)
Test Disaster Recovery Plan	Generally involves the actual recovery and operation

	of the covered systems at their recovery site for a defined period. While unannounced tests are ideal, normal logistics of reserving the test center, budgeting for travel, overtime, etc. means these tests are always announced.
--	--

1.3.6. Event Management



Reference(s):

- IT Cyber Security Communication COOP Event Management.html

Links to Z22 (listed alphabetically)	
Name	Description
Declare Disaster Events and Respond to Call for Help	Generally involves the actual recovery and operation of the covered systems at their recovery site for a defined period. This is a worse case scenario where the initial emergency response was unable to avoid or protect the facility from damage or destruction.
Perform Change Management	Involves the tasks associated with the assessment, scheduling, implementing and reviewing of all changes. This activity produces the approval or disapproval to implement a change.
Perform Configuration Management	This activity covers the identification of all

	<p>significant components within the IT infrastructure as well as the relationship between components. The management of the associated data enables all other processes to function more effectively and efficiently.</p>
Perform Crisis Control during Events	<p>The crisis control function provides overall coordination of the plan and communications to internal and external entities during an event. The crisis control team generally makes the decision to declare a disaster and begin activating the recovery plan.</p>
Perform Incident Management	<p>Involves the tasks associated with restoring to normal service as quickly as possible following the loss of service, in order to minimize the adverse impact on business operations, thus ensuring that the best possible level of service quality and availability are maintained.</p>
Perform Problem Management	<p>Involves the tasks associated with minimizing the adverse impact of incidents and problems on the business. These may be caused by errors within the IT infrastructure. In addition, the task prevents recurrence of incidents related to these errors. This activity may be reactive to an incident that has occurred or proactive in resolving the root cause of an incident before it reoccurs.</p>
Perform Release Management	<p>This activity is closely related to change and configuration management and involves all tasks associated with planning, designing, building and testing hardware and software to create a set of release components for the production environment.</p>
Respond to Initial Events	<p>Throughout the year, emergency events covered in the plan may occur, these events will be responded to following the plan. The responses will be designed to contain the event and to avoid wherever possible the escalation of the event. A part of the process also includes assessing the damage and advising the crisis control managers of the status of the operation.</p>

1.3.7. Maintaining Plans



Reference(s):

- IT Cyber Security Communication COOP Maintaining Plans.html

Links to Z22 (listed alphabetically)	
Name	Description
Perform Post-event Lessons Learned Reviews	Throughout the year, emergency events covered in the plan may occur. These events will be responded to following the plan. Following completion of the emergency event, a post analysis of the plan components exercised is accomplished to identify where modifications are needed
Perform Post- test Lessons Learned Reviews	Following planned tests, whether tabletop or full dress rehearsals, the teams will meet to identify where improvements can be made in the process.
Perform Routine Plan Maintenance	Throughout the year as systems, supporting organizations, contracts and vendors change, these changes will need to be made to the plans. These changes generally involve updating lists that are used to support the action items on the plans.

1.4. Enterprise Architecture Process

Process Sequence Diagram TBD.