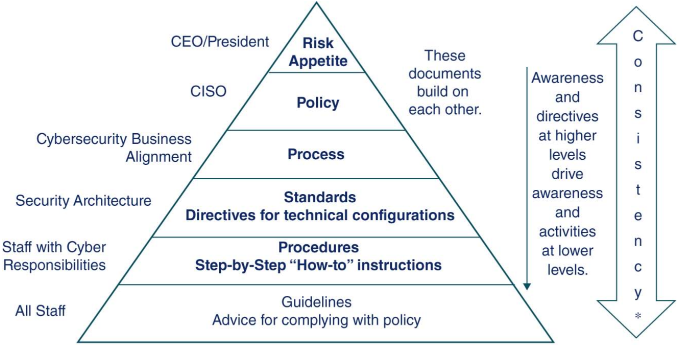


CEO/President — **Risk Appetite**

CISO — **Policy**

Cybersecurity Business Alignment — **Process**

Security Architecture — **Standards Directives for technical configurations**

Staff with Cyber Responsibilities — **Procedures Step-by-Step “How-to” instructions**

All Staff — Guidelines Advice for complying with policy

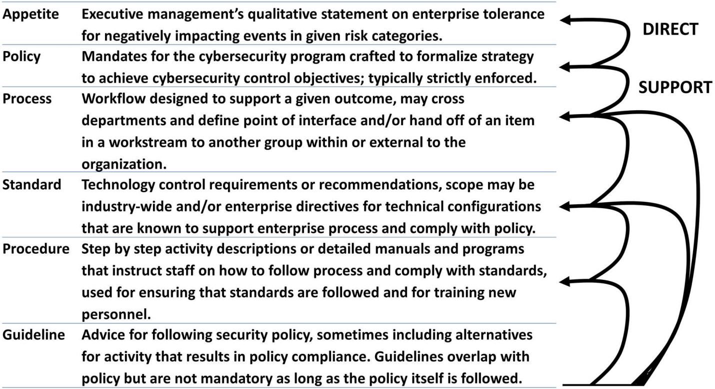
These documents build on each other.

Awareness and directives at higher levels drive awareness and activities at lower levels.

Consistency*

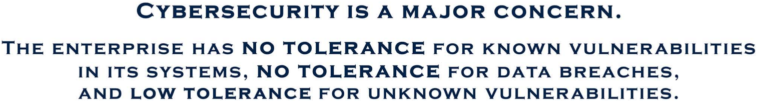
**In addition to internal documents, consistency must extend to legal obligations and contractual requirements.*

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.1



Appetite	Executive management's qualitative statement on enterprise tolerance for negatively impacting events in given risk categories.
Policy	Mandates for the cybersecurity program crafted to formalize strategy to achieve cybersecurity control objectives; typically strictly enforced.
Process	Workflow designed to support a given outcome, may cross departments and define point of interface and/or hand off of an item in a workstream to another group within or external to the organization.
Standard	Technology control requirements or recommendations, scope may be industry-wide and/or enterprise directives for technical configurations that are known to support enterprise process and comply with policy.
Procedure	Step by step activity descriptions or detailed manuals and programs that instruct staff on how to follow process and comply with standards, used for ensuring that standards are followed and for training new personnel.
Guideline	Advice for following security policy, sometimes including alternatives for activity that results in policy compliance. Guidelines overlap with policy but are not mandatory as long as the policy itself is followed.

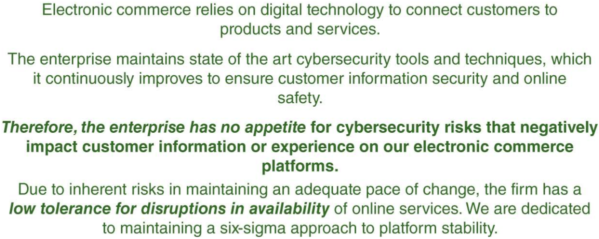
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.2



Cybersecurity is a major concern.

The enterprise has **NO TOLERANCE** for known vulnerabilities
in its systems, **NO TOLERANCE** for data breaches,
and **low tolerance** for unknown vulnerabilities.

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.3



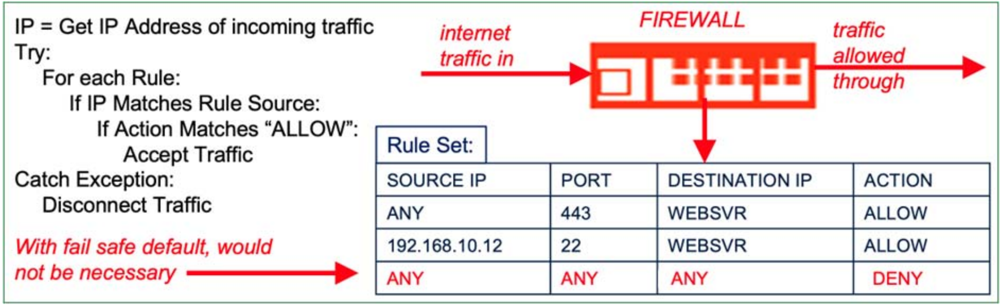
Electronic commerce relies on digital technology to connect customers to products and services.

The enterprise maintains state of the art cybersecurity tools and techniques, which it continuously improves to ensure customer information security and online safety.

***Therefore, the enterprise has no appetite* for cybersecurity risks that negatively impact customer information or experience on our electronic commerce platforms.**

Due to inherent risks in maintaining an adequate pace of change, the firm has a ***low tolerance for disruptions in availability*** of online services. We are dedicated to maintaining a six-sigma approach to platform stability.

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.4



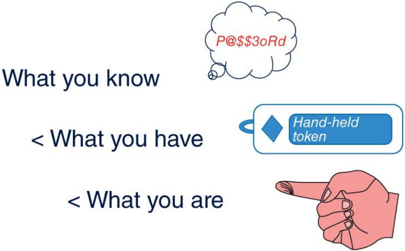
```
IP = Get IP Address of incoming traffic
Try:
    For each Rule:
        If IP Matches Rule Source:
            If Action Matches "ALLOW":
                Accept Traffic
Catch Exception:
    Disconnect Traffic
```

With fail safe default, would not be necessary

Rule Set:

SOURCE IP	PORT	DESTINATION IP	ACTION
ANY	443	WEBSVR	ALLOW
192.168.10.12	22	WEBSVR	ALLOW
ANY	ANY	ANY	DENY

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.5

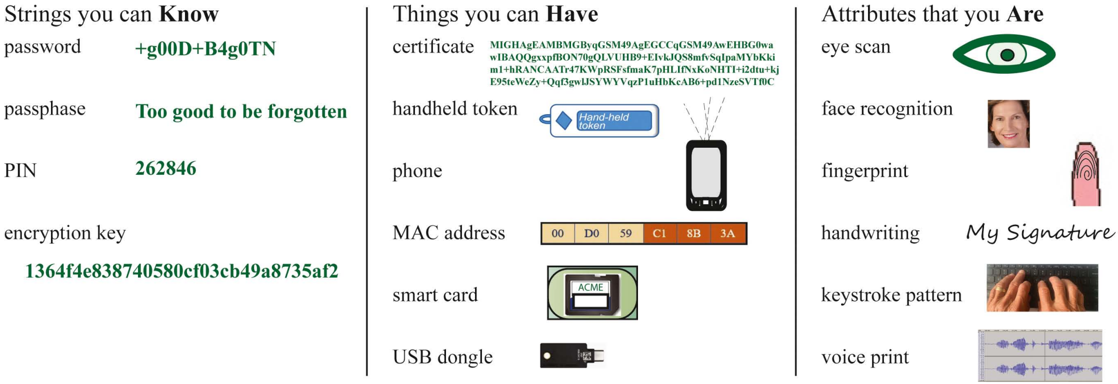


What you know

< What you have

< What you are

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.6



Strings you can **Know**

password +g00D+B4g0TN

passphase Too good to be forgotten

PIN 262846

encryption key

1364f4e838740580cf03cb49a8735af2

Things you can **Have**

certificate MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wa
wIBAQQgxxpfBON70gQLVUHB9+EIvkJQS8mfvSqIpaMYbKki
m1+hRANCAATr47KWpRSFsfmaK7pHLIfNxKoNHTI+i2dtu+kj
E95teWeZy+Qqf3gwlJSYWYVqzP1uHbKcAB6+pd1NzeSVTf0C

handheld token

phone

MAC address

smart card

USB dongle

Attributes that you **Are**

eye scan

face recognition

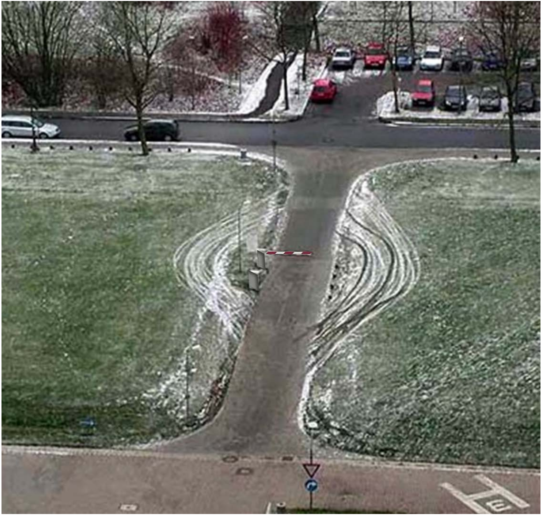
fingerprint

handwriting

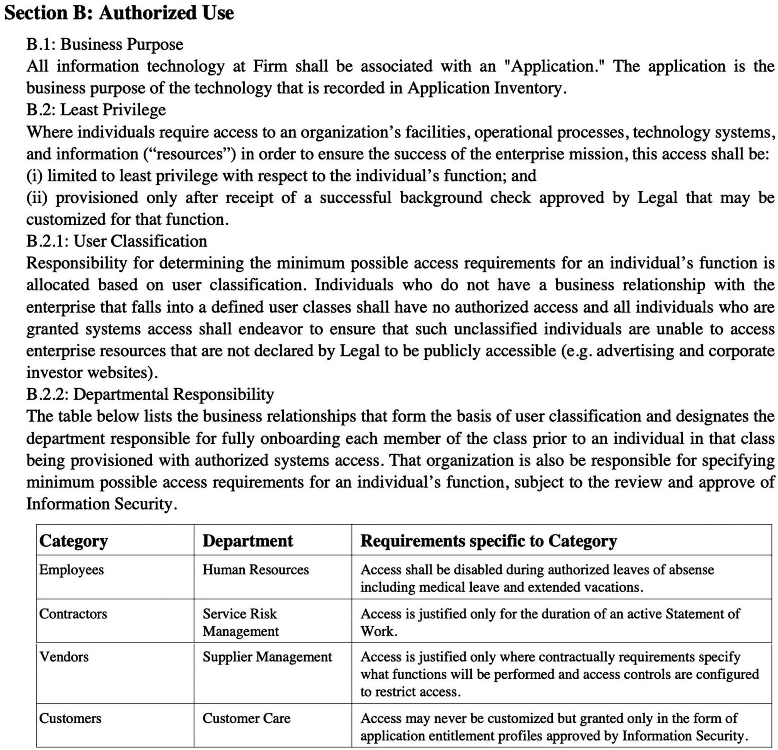
keystroke pattern

voice print

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.7



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.8



Section B: Authorized Use

B.1: Business Purpose

All information technology at Firm shall be associated with an "Application." The application is the business purpose of the technology that is recorded in Application Inventory.

B.2: Least Privilege

Where individuals require access to an organization's facilities, operational processes, technology systems, and information ("resources") in order to ensure the success of the enterprise mission, this access shall be:

(i) limited to least privilege with respect to the individual's function; and

(ii) provisioned only after receipt of a successful background check approved by Legal that may be customized for that function.

B.2.1: User Classification

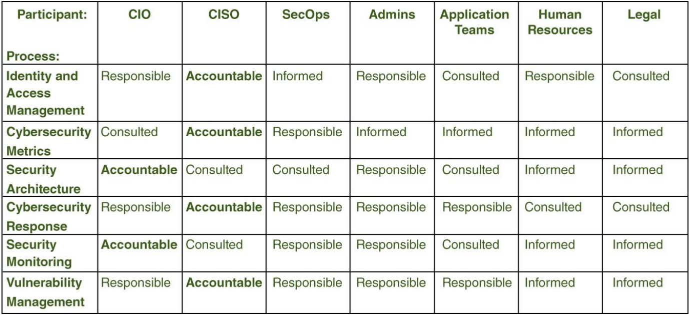
Responsibility for determining the minimum possible access requirements for an individual's function is allocated based on user classification. Individuals who do not have a business relationship with the enterprise that falls into a defined user classes shall have no authorized access and all individuals who are granted systems access shall endeavor to ensure that such unclassified individuals are unable to access enterprise resources that are not declared by Legal to be publicly accessible (e.g. advertising and corporate investor websites).

B.2.2: Departmental Responsibility

The table below lists the business relationships that form the basis of user classification and designates the department responsible for fully onboarding each member of the class prior to an individual in that class being provisioned with authorized systems access. That organization is also be responsible for specifying minimum possible access requirements for an individual's function, subject to the review and approve of Information Security.

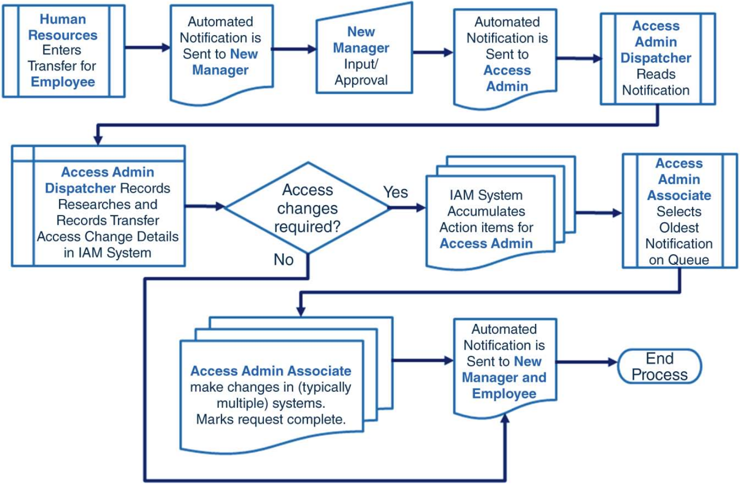
Category	Department	Requirements specific to Category
Employees	Human Resources	Access shall be disabled during authorized leaves of absense including medical leave and extended vacations.
Contractors	Service Risk Management	Access is justified only for the duration of an active Statement of Work.
Vendors	Supplier Management	Access is justified only where contractually requirements specify what functions will be performed and access controls are configured to restrict access.
Customers	Customer Care	Access may never be customized but granted only in the form of application entitlement profiles approved by Information Security.

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.9

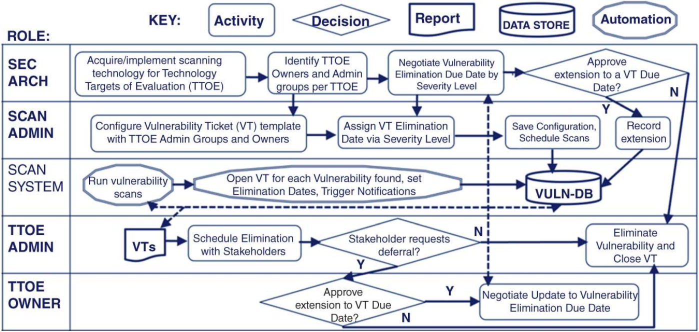


Participant: **Process:**	**CIO**	**CISO**	**SecOps**	**Admins**	**Application Teams**	**Human Resources**	**Legal**
Identity and Access Management	Responsible	**Accountable**	Informed	Responsible	Consulted	Responsible	Consulted
Cybersecurity Metrics	Consulted	**Accountable**	Responsible	Informed	Informed	Informed	Informed
Security Architecture	**Accountable**	Consulted	Consulted	Responsible	Consulted	Informed	Informed
Cybersecurity Response	Responsible	**Accountable**	Responsible	Responsible	Responsible	Consulted	Consulted
Security Monitoring	**Accountable**	Consulted	Responsible	Responsible	Consulted	Informed	Informed
Vulnerability Management	Responsible	**Accountable**	Responsible	Responsible	Responsible	Informed	Informed

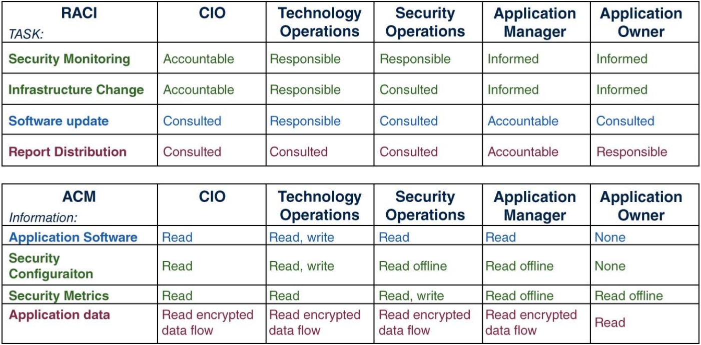
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.10


Human Resources Enters Transfer for Employee
Automated Notification is Sent to New Manager
New Manager Input/ Approval
Automated Notification is Sent to Access Admin
Access Admin Dispatcher Reads Notification
Access Admin Dispatcher Records Researches and Records Transfer Access Change Details in IAM System
Access changes required?
Yes
No
IAM System Accumulates Action items for Access Admin
Access Admin Associate Selects Oldest Notification on Queue
Access Admin Associate make changes in (typically multiple) systems. Marks request complete.
Automated Notification is Sent to New Manager and Employee
End Process

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.11


KEY:
Activity
Decision
Report
DATA STORE
Automation
ROLE:
SEC ARCH
SCAN ADMIN
SCAN SYSTEM
TTOE ADMIN
TTOE OWNER
Acquire/implement scanning technology for Technology Targets of Evaluation (TTOE)
Identify TTOE Owners and Admin groups per TTOE
Negotiate Vulnerability Elimination Due Date by Severity Level
Approve extension to a VT Due Date?
N
Y
Configure Vulnerability Ticket (VT) template with TTOE Admin Groups and Owners
Assign VT Elimination Date via Severity Level
Save Configuration, Schedule Scans
Record extension
Run vulnerability scans
Open VT for each Vulnerability found, set Elimination Dates, Trigger Notifications
VULN-DB
VTs
Schedule Elimination with Stakeholders
Stakeholder requests deferral?
N
Y
Eliminate Vulnerability and Close VT
Approve extension to VT Due Date?
Y
N
Negotiate Update to Vulnerability Elimination Due Date

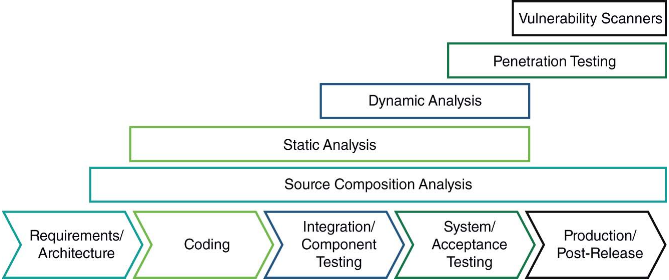
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.12



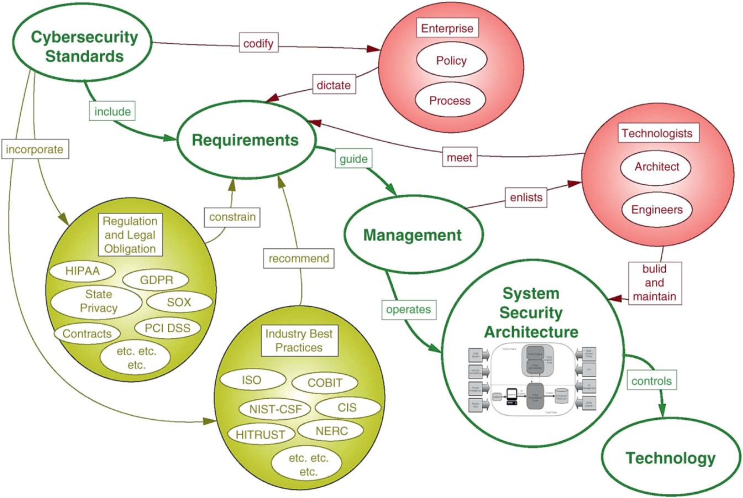
RACI *TASK:*	CIO	Technology Operations	Security Operations	Application Manager	Application Owner
Security Monitoring	Accountable	Responsible	Responsible	Informed	Informed
Infrastructure Change	Accountable	Responsible	Consulted	Informed	Informed
Software update	Consulted	Responsible	Consulted	Accountable	Consulted
Report Distribution	Consulted	Consulted	Consulted	Accountable	Responsible

ACM *Information:*	CIO	Technology Operations	Security Operations	Application Manager	Application Owner
Application Software	Read	Read, write	Read	Read	None
Security Configuraiton	Read	Read, write	Read offline	Read offline	None
Security Metrics	Read	Read	Read, write	Read offline	Read offline
Application data	Read encrypted data flow	Read encrypted data flow	Read encrypted data flow	Read encrypted data flow	Read

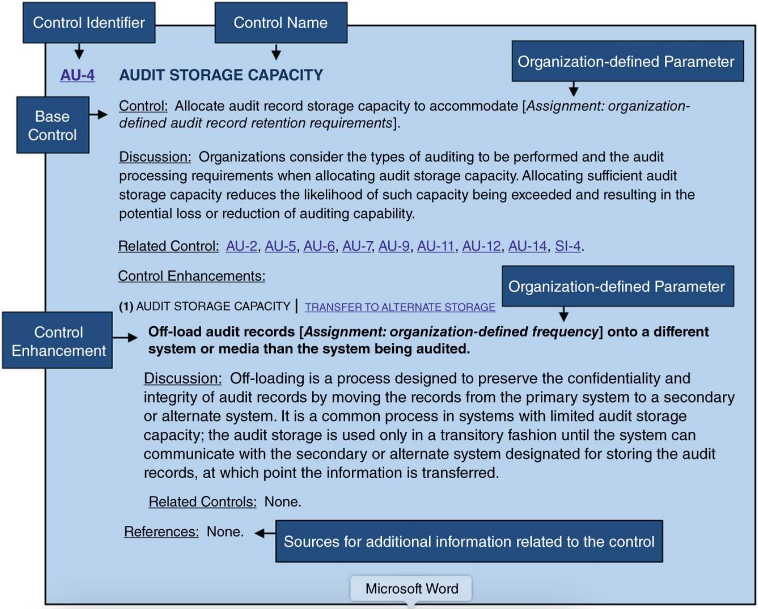
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.13


Vulnerability Scanners
Penetration Testing
Dynamic Analysis
Static Analysis
Source Composition Analysis
Requirements/ Architecture
Coding
Integration/ Component Testing
System/ Acceptance Testing
Production/ Post-Release

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.14



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.15



Control Identifier
Control Name
Organization-defined Parameter
Base Control
Organization-defined Parameter
Control Enhancement
Sources for additional information related to the control
Microsoft Word

AU-4 AUDIT STORAGE CAPACITY

Control: Allocate audit record storage capacity to accommodate [*Assignment: organization-defined audit record retention requirements*].

Discussion: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Related Control: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Control Enhancements:

(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

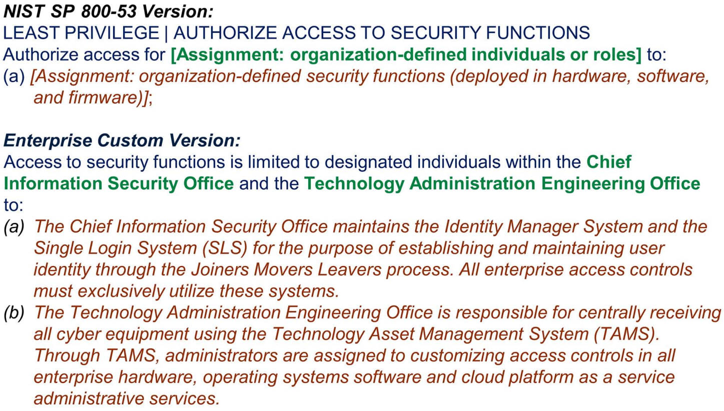
Off-load audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

Discussion: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary system to a secondary or alternate system. It is a common process in systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

Related Controls: None.

References: None.

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.16



NIST SP 800-53 Version:

LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Authorize access for **[Assignment: organization-defined individuals or roles]** to:

(a) *[Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]*;

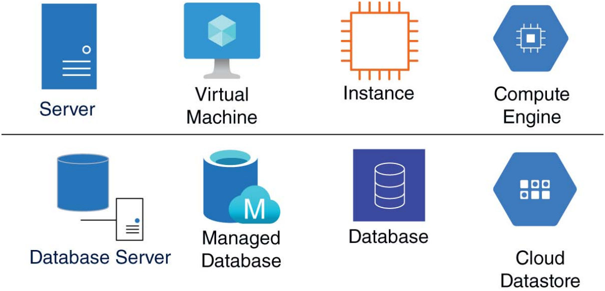
Enterprise Custom Version:

Access to security functions is limited to designated individuals within the **Chief Information Security Office** and the **Technology Administration Engineering Office** to:

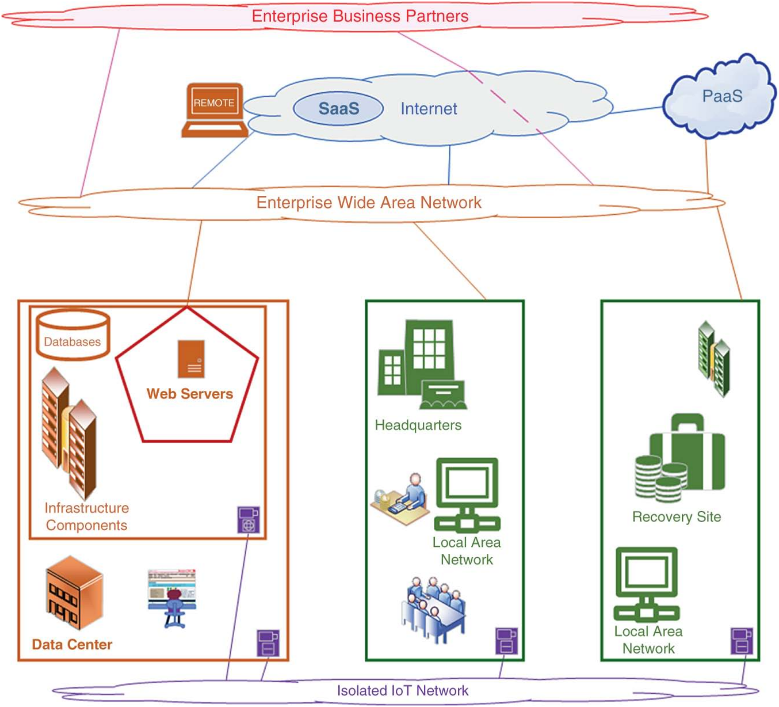
(a) The Chief Information Security Office maintains the Identity Manager System and the Single Login System (SLS) for the purpose of establishing and maintaining user identity through the Joiners Movers Leavers process. All enterprise access controls must exclusively utilize these systems.

(b) The Technology Administration Engineering Office is responsible for centrally receiving all cyber equipment using the Technology Asset Management System (TAMS). Through TAMS, administrators are assigned to customizing access controls in all enterprise hardware, operating systems software and cloud platform as a service administrative services.

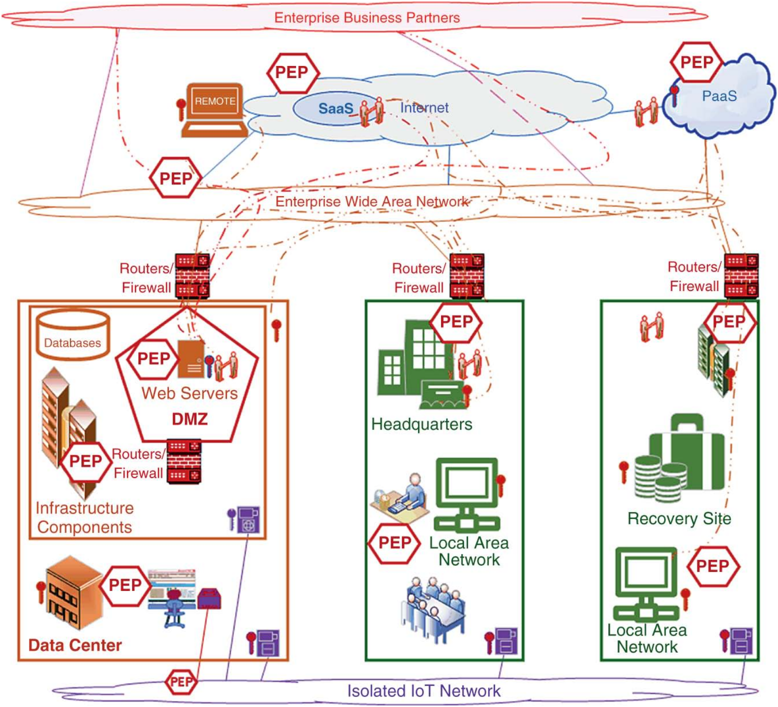
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.17



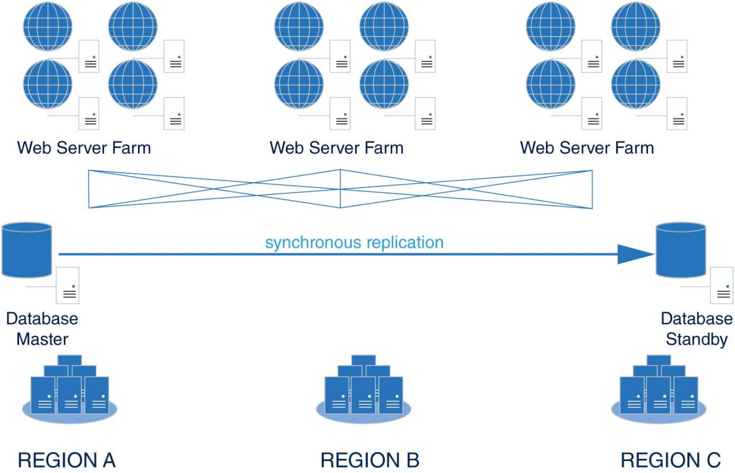
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.18



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.19



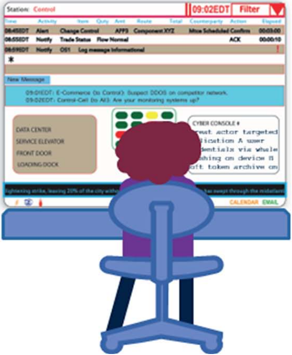
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.20



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.21

The Security Operations Center Analyst:

1. Select the highest priority alert in the queue
2. Ascertain context:
   2.a. app or data in alert, search application registry for app/data owner
   2.b. device or IP in alert, search asset inventory for device and/or network owner
3. If the priority is “critical”, convene call with supervisor and app/data/device/net owners
4. Use data in alert to distinguish between anomaly and intrusion:
   3.a. if intrusion or cannot tell, make a note in the log asking supervisor for instruction
   3.b. anomaly, place alert on list for end-of-shift call with app/data/device/net owners


Station: Control
09:02EDT
Filter
Time Activity Item Qnty Amt Route Total Counterparty Action Elapsed
08:45EDT Alert Change Control APP3 Component XYZ Miss Scheduled Confirm 00:03:00
08:55EDT Notify Trade Status Flow Normal ACK 00:00:10
08:59EDT Notify OS1 Log message Informational
New Message
09:01EDT: E-Commerce (to Control): Suspect DDOS on competitor network.
09:02EDT: Control-Call (to All): Are your monitoring systems up?
DATA CENTER
SERVICE ELEVATOR
FRONT DOOR
LOADING DOCK
CYBER CONSOLE #
reat actor targeted
lication A user
dentials via whale
shing on device B
oft token archive on
lightening strike, leaving 20% of the city witho
has swept through the midatlantic
CALENDAR EMAIL

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.22

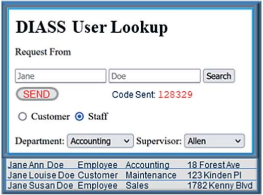
The guard at the gate:

1. Ask visitor for identification and staff they are visiting
2. Search building access system for visitor appointment
   - 2.a. If visit is expected, notify staff in appointment
   - 2.b. If not, explain to the visitor that staff must call security to authorize admission
3. If no staff authorization, save visitor ID and photo in log

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.23

Service Desk personnel will follow these instructions:

1. Receive phone call for assistance. Request caller's first and last name. Ask the caller if they are a customer.
2. Type caller's first and last names into the corresponding search screen fields on the Department Identity and Access Security System (DIASS). If the caller is a customer, select the button to the right of the word "CUSTOMER." Select "SEARCH".
3. Matching records will appear in a search result table under the search form. If more than one record is in the table, ask the caller for more information with which to select the correct record.
   a. If the caller is a customer, ask: "What service do you use?"
   b. If the caller is not a customer, ask: "What department do you work for?"
4. Select the answer to question 3 from the "Department" dropdown list.
5. The list of matching records will again appear in the table below. If there are still multiple, ask the caller their middle name or address to find a unique record.
6. If no record in the identity management system corresponds to the caller, refer the caller to their sales associate or supervisor and politely end the call. **STOP HERE**
7. Select the **SEND** button under the user first name, then ask the caller to recite the code sent.
8. If the caller cannot recite the code, refer the caller to their sales associate or supervisor and politely end the call. **STOP HERE**



DIASS User Lookup

Request From

Jane Doe

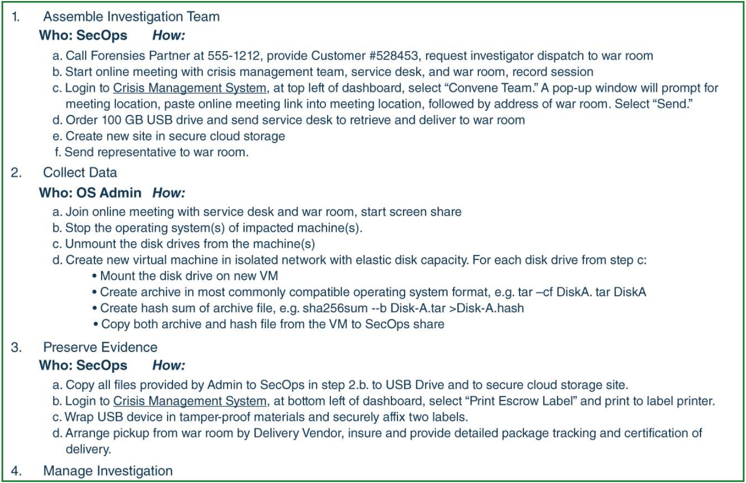
Code Sent: 128329

○ Customer ● Staff

Department: Accounting Supervisor: Allen

Jane Ann Doe	Employee	Accounting	18 Forest Ave
Jane Louise Doe	Customer	Maintenance	123 Kinden Pl
Jane Susan Doe	Employee	Sales	1782 Kenny Blvd

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.24



1. Assemble Investigation Team

Who: SecOps ***How:***

a. Call Forensies Partner at 555-1212, provide Customer #528453, request investigator dispatch to war room
b. Start online meeting with crisis management team, service desk, and war room, record session
c. Login to <u>Crisis Management System</u>, at top left of dashboard, select "Convene Team." A pop-up window will prompt for meeting location, paste online meeting link into meeting location, followed by address of war room. Select "Send."
d. Order 100 GB USB drive and send service desk to retrieve and deliver to war room
e. Create new site in secure cloud storage
f. Send representative to war room.

2. Collect Data

Who: OS Admin ***How:***

a. Join online meeting with service desk and war room, start screen share
b. Stop the operating system(s) of impacted machine(s).
c. Unmount the disk drives from the machine(s)
d. Create new virtual machine in isolated network with elastic disk capacity. For each disk drive from step c:

- Mount the disk drive on new VM
- Create archive in most commonly compatible operating system format, e.g. tar –cf DiskA. tar DiskA
- Create hash sum of archive file, e.g. sha256sum --b Disk-A.tar >Disk-A.hash
- Copy both archive and hash file from the VM to SecOps share

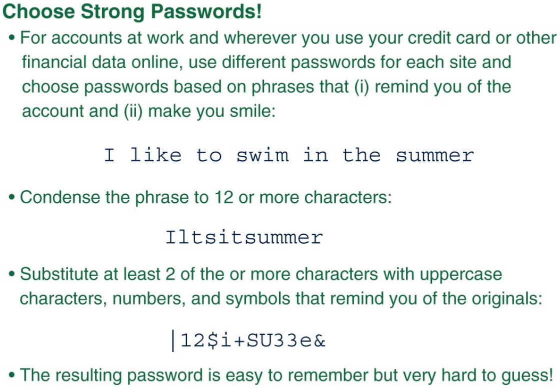
3. Preserve Evidence

Who: SecOps ***How:***

a. Copy all files provided by Admin to SecOps in step 2.b. to USB Drive and to secure cloud storage site.
b. Login to <u>Crisis Management System</u>, at bottom left of dashboard, select "Print Escrow Label" and print to label printer.
c. Wrap USB device in tamper-proof materials and securely affix two labels.
d. Arrange pickup from war room by Delivery Vendor, insure and provide detailed package tracking and certification of delivery.

4. Manage Investigation

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.25



Choose Strong Passwords!

- For accounts at work and wherever you use your credit card or other financial data online, use different passwords for each site and choose passwords based on phrases that (i) remind you of the account and (ii) make you smile:

```
I like to swim in the summer
```

- Condense the phrase to 12 or more characters:

```
Iltsitsummer
```

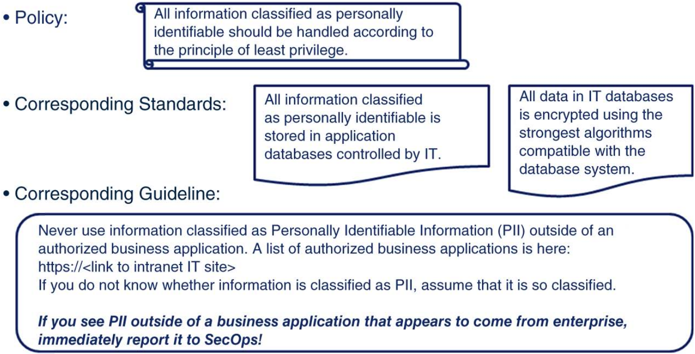
- Substitute at least 2 of the or more characters with uppercase characters, numbers, and symbols that remind you of the originals:

```
|12$i+SU33e&
```

- The resulting password is easy to remember but very hard to guess!

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.26

How Enterprise Cybersecurity Guidelines Help



- Policy:

All information classified as personally identifiable should be handled according to the principle of least privilege.

- Corresponding Standards:

All information classified as personally identifiable is stored in application databases controlled by IT.

All data in IT databases is encrypted using the strongest algorithms compatible with the database system.

- Corresponding Guideline:

Never use information classified as Personally Identifiable Information (PII) outside of an authorized business application. A list of authorized business applications is here: https://<link to intranet IT site>
If you do not know whether information is classified as PII, assume that it is so classified.

If you see PII outside of a business application that appears to come from enterprise, immediately report it to SecOps!

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 4.27