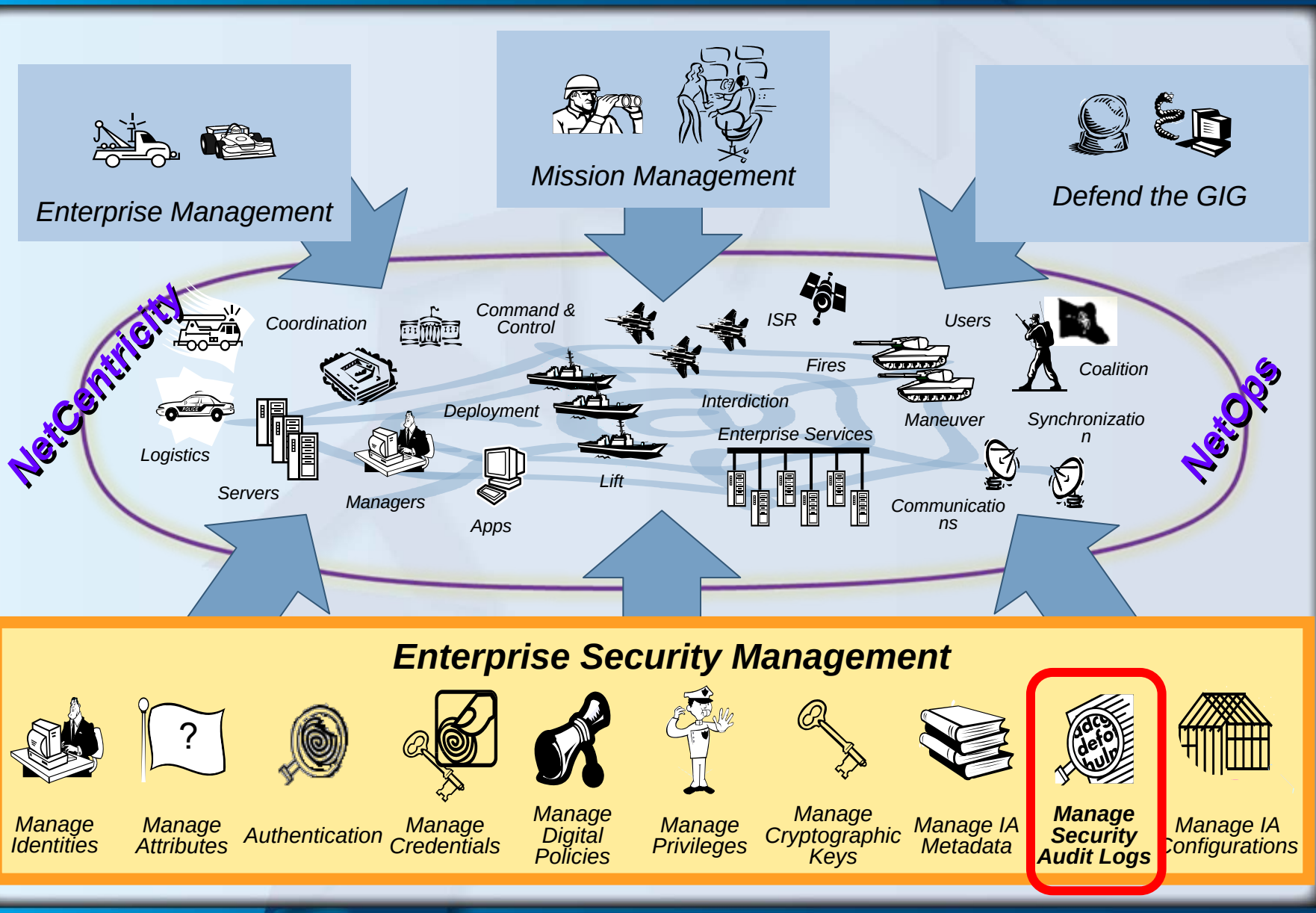
Enterprise-Wide Audit-Data Management

Enterprise Security Management
Special Program Office (NSA/I5E)

Lloyd E Lutz Jr
Booz Allen Hamilton

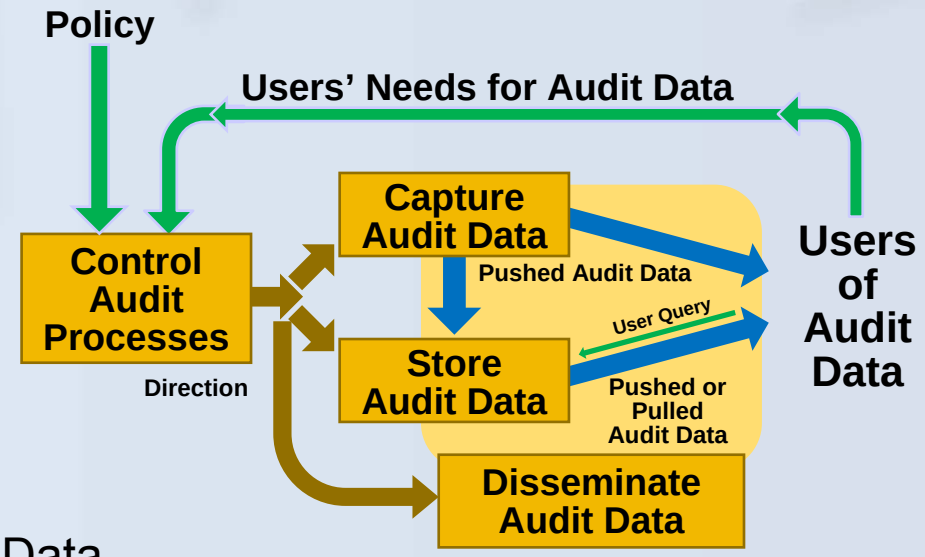
27 October 2009

Enterprise Security Management Overview



Scope of Audit-Data Management

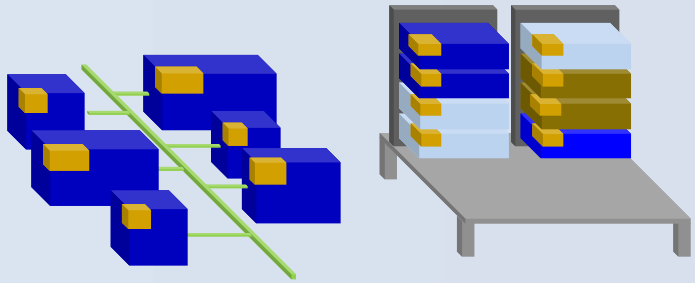
- **Audit-Data Management is one of 10 Enterprise Security Management Functions**
- **Four Key Audit Functions**
  - **Capture Audit Data**
  - **Store Audit Data**
  - **Disseminate Audit Data**
  - **Control Audit Processes**
    - Direction to Devices
    - Direction for Storage of Audit Data
    - Direction of Dissemination of Audit Data
    - Overall Management of Processes to Satisfy Users' Needs for Audit Data



Hierarchy of Enterprise-Wide Management of Audit Data

Individual Devices

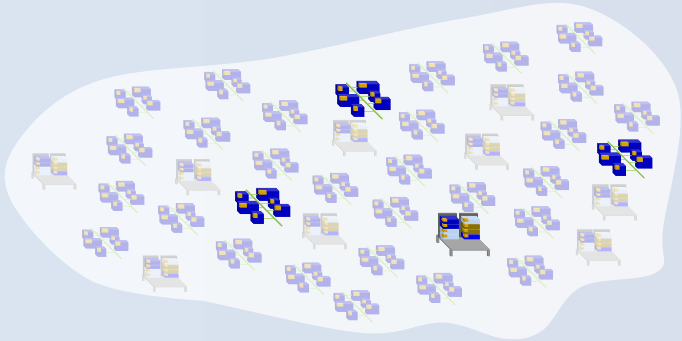
- **Part of LAN or Platform**
- **Have Audit Capabilities**
  - Detect Device Events
  - *Capture Audit Data*
  - Hold Audit Data
  - Report Audit Data



Hierarchy of Enterprise-Wide Management of Audit Data

Individual Devices

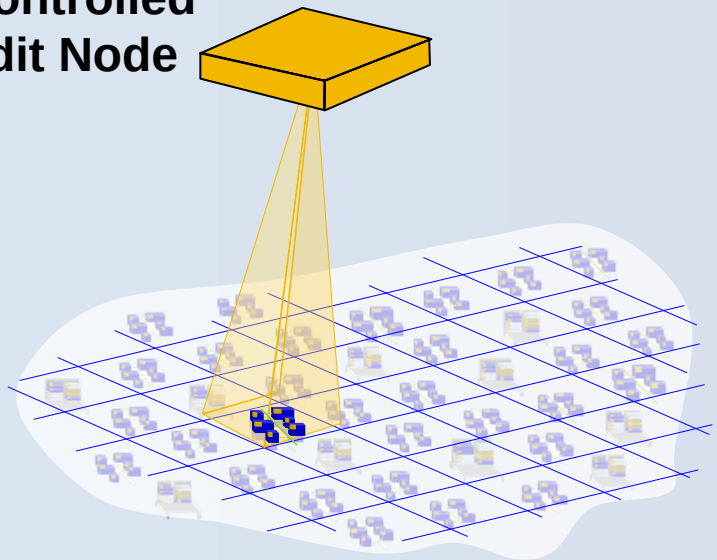
- **Part of LAN or Platform**
- **Have Audit Capabilities**
  - Detect Device Events
  - *Capture Audit Data*
  - Hold Audit Data
  - Report Audit Data



Hierarchy of Enterprise-Wide Management of Audit Data

Local Audit Node

- **Each Device Is Controlled by One Local Audit Node**



Individual Devices

- **Part of LAN or Platform**
- **Have Audit Capabilities**
  - Detect Device Events
  - *Capture Audit Data*
  - Hold Audit Data
  - Report Audit Data

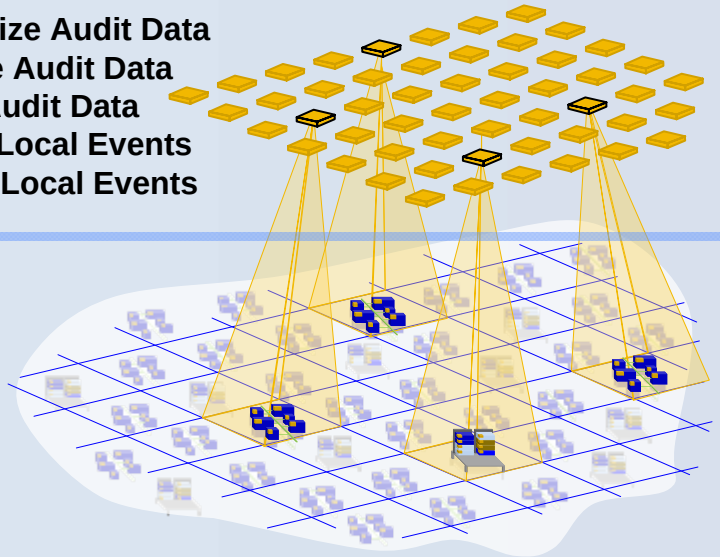
Hierarchy of Enterprise-Wide Management of Audit Data

Local Audit Nodes (Tier-3)

- **Direct Auditing Devices**
  - Coordinate with Peers
  - Verify Audit Configuration
  - Receive Audit Data from Devices
- **Normalize Audit Data**
- **Reduce Audit Data**
- **Store Audit Data**
- **Detect Local Events**
- **Report Local Events**

Individual Devices

- Part of LAN or Platform
- **Detect Device Events**
- ***Capture Audit Data***
- **Hold Audit Data**
- **Report Audit Data**
- Directed by One Local Audit Node



Hierarchy of Enterprise-Wide Management of Audit Data

Region-Organization Audit (Tier-2)

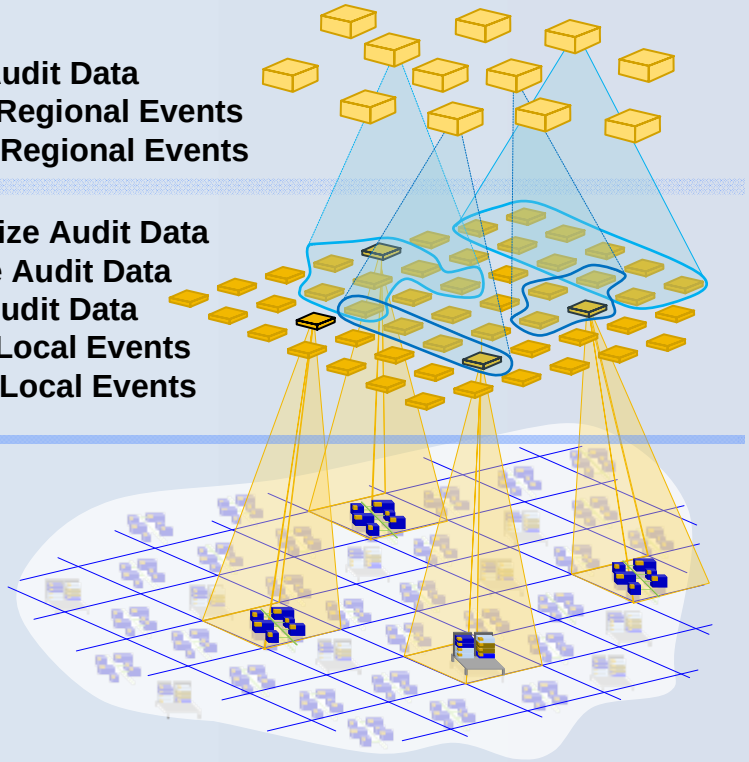
- **Plan & Direct Regional Audit Actions**
- **Direct Sets of Local Audit Nodes**
  - **Coordinate with Peers (NetOps)**
  - **Verify Direction Compliance**
  - **Receive Event Reports**
  - **Retrieve Audit Data**
- **Store Audit Data**
- **Detect Regional Events**
- **Report Regional Events**

Local Audit Nodes (Tier-3)

- **Direct Auditing Devices**
  - Coordinate with Peers
  - Verify Audit Configuration
  - Receive Audit Data from Devices
- **Normalize Audit Data**
- **Reduce Audit Data**
- **Store Audit Data**
- **Detect Local Events**
- **Report Local Events**

Individual Devices

- Part of LAN or Platform
- **Detect Device Events**
- ***Capture Audit Data***
- **Hold Audit Data**
- **Report Audit Data**
- Directed by One Local Audit Node



Hierarchy of Enterprise-Wide Management of Audit Data

CC-Service-Agency Audit (Tier-1)

- **Plan & Direct Auditing**
- **Coordinate with Peers (NetOps)**
- **Assess Audit Effectiveness**
- **Audit Capability Development**
- **Receive Event Reports**
- **Store Event Data**
- **Detect CC/S/A & Enterprise Events**
- **Report Events**

Region-Organization Audit (Tier-2)

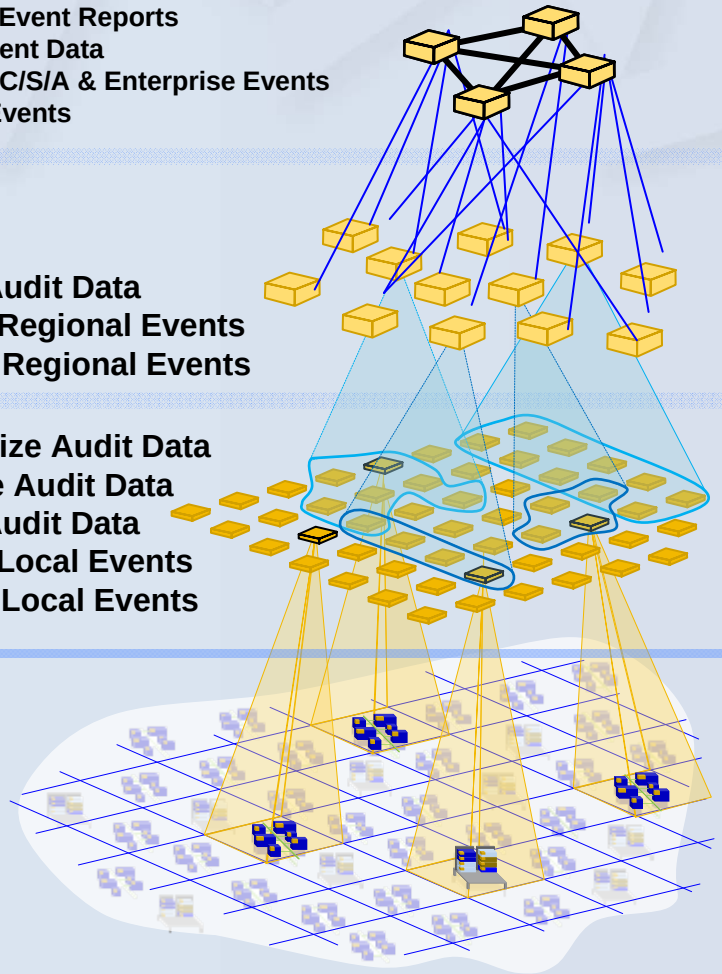
- **Plan & Direct Regional Audit Actions**
- **Direct Sets of Local Audit Nodes**
  - **Coordinate with Peers (NetOps)**
  - **Verify Direction Compliance**
  - **Receive Event Reports**
  - **Retrieve Audit Data**
- **Store Audit Data**
- **Detect Regional Events**
- **Report Regional Events**

Local Audit Nodes (Tier-3)

- **Direct Auditing Devices**
  - Coordinate with Peers
  - Verify Audit Configuration
  - Receive Audit Data from Devices
- **Normalize Audit Data**
- **Reduce Audit Data**
- **Store Audit Data**
- **Detect Local Events**
- **Report Local Events**

Individual Devices

- Part of LAN or Platform
- **Detect Device Events**
- ***Capture Audit Data***
- **Hold Audit Data**
- **Report Audit Data**
- Directed by One Local Audit Node



Hierarchy of Enterprise-Wide Management of Audit Data

Enterprise

- **Plan & Direct Auditing Operations**
- **Enterprise Audit Policy**
- **Assess Audit Effectiveness**
- **Audit Capability Requirements**
- **Receive Reports**
- **Federate with Other Enterprises**

CC-Service-Agency Audit (Tier-1)

- **Plan & Direct Auditing**
- **Coordinate with Peers (NetOps)**
- **Assess Audit Effectiveness**
- **Audit Capability Development**
- **Receive Event Reports**
- **Store Event Data**
- **Detect CC/S/A & Enterprise Events**
- **Report Broad-Scope Events**

Region-Organization Audit (Tier-2)

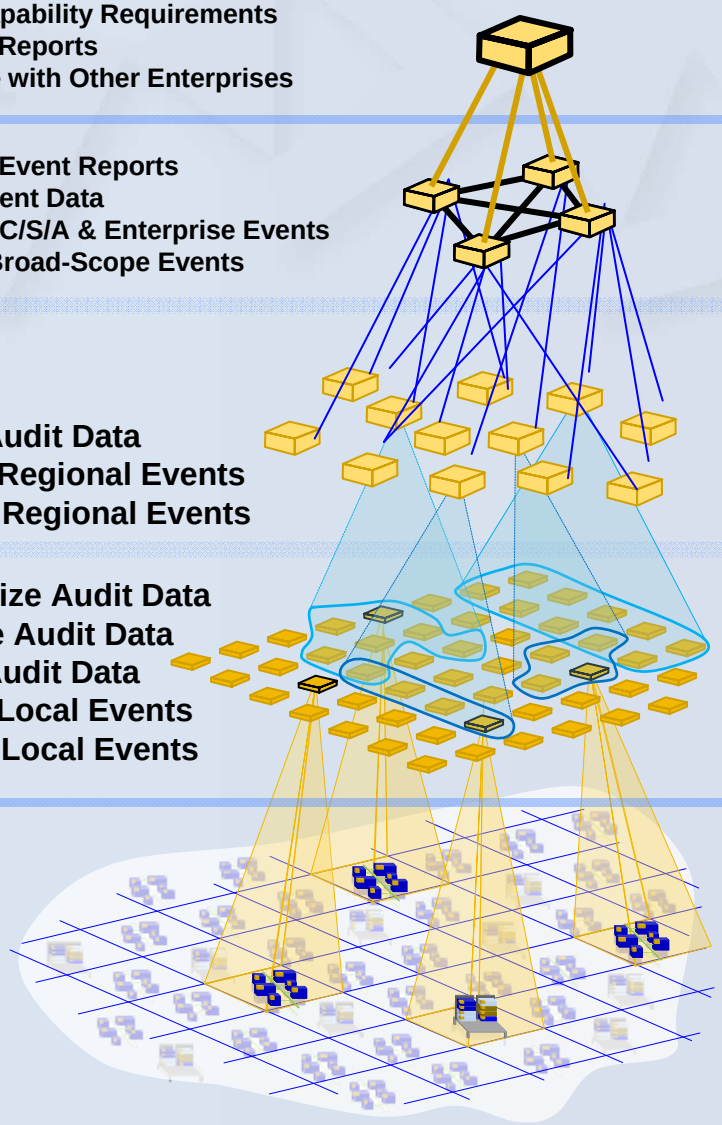
- **Plan & Direct Regional Audit Actions**
- **Direct Sets of Local Audit Nodes**
  - **Coordinate with Peers (NetOps)**
  - **Verify Direction Compliance**
  - **Receive Event Reports**
  - **Retrieve Audit Data**
- **Store Audit Data**
- **Detect Regional Events**
- **Report Regional Events**

Local Audit Nodes (Tier-3)

- **Direct Auditing Devices**
  - Coordinate with Peers
  - Verify Audit Configuration
  - Receive Audit Data from Devices
- **Normalize Audit Data**
- **Reduce Audit Data**
- **Store Audit Data**
- **Detect Local Events**
- **Report Local Events**

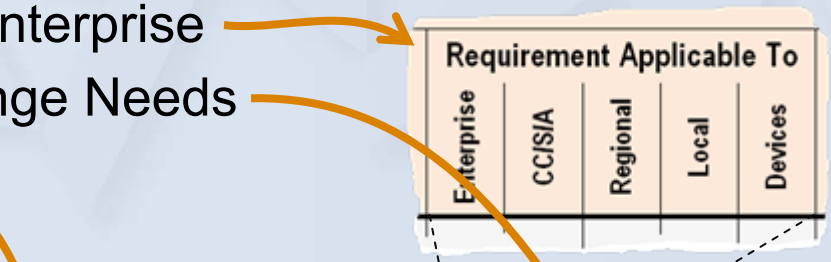
Individual Devices

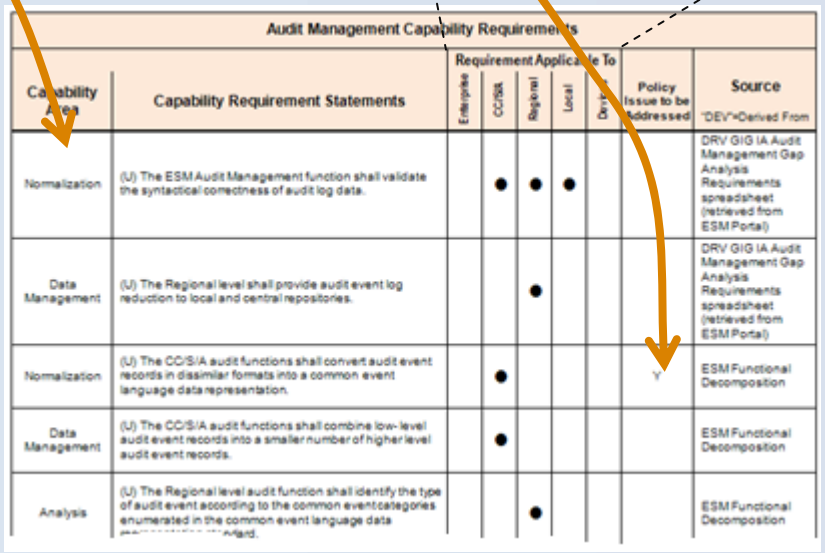
- Part of LAN or Platform
- **Detect Device Events**
- ***Capture Audit Data***
- **Hold Audit Data**
- **Report Audit Data**
- Directed by One Local Audit Node



Compilation of High-Level Requirements

- **Seeking Current Requirements Documents**
  - *Initial* Allocation to Level Within Enterprise
  - *Initial* Identification of Policy Change Needs
  - Binning by Capability Area
- **Ongoing Efforts:**
  - Collection of Requirements
  - Identification of Conflicts
  - Identification of Needed Policy
  - Community Review & Feedback



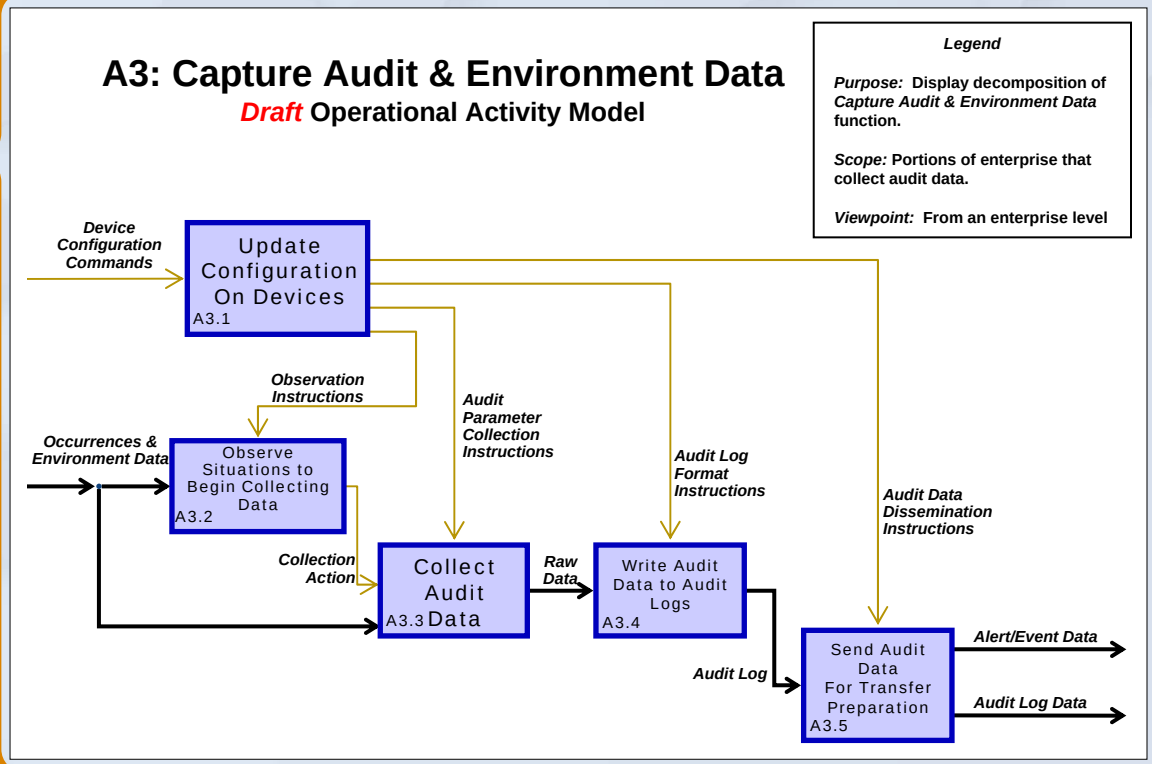


Audit Management Capability Requirements

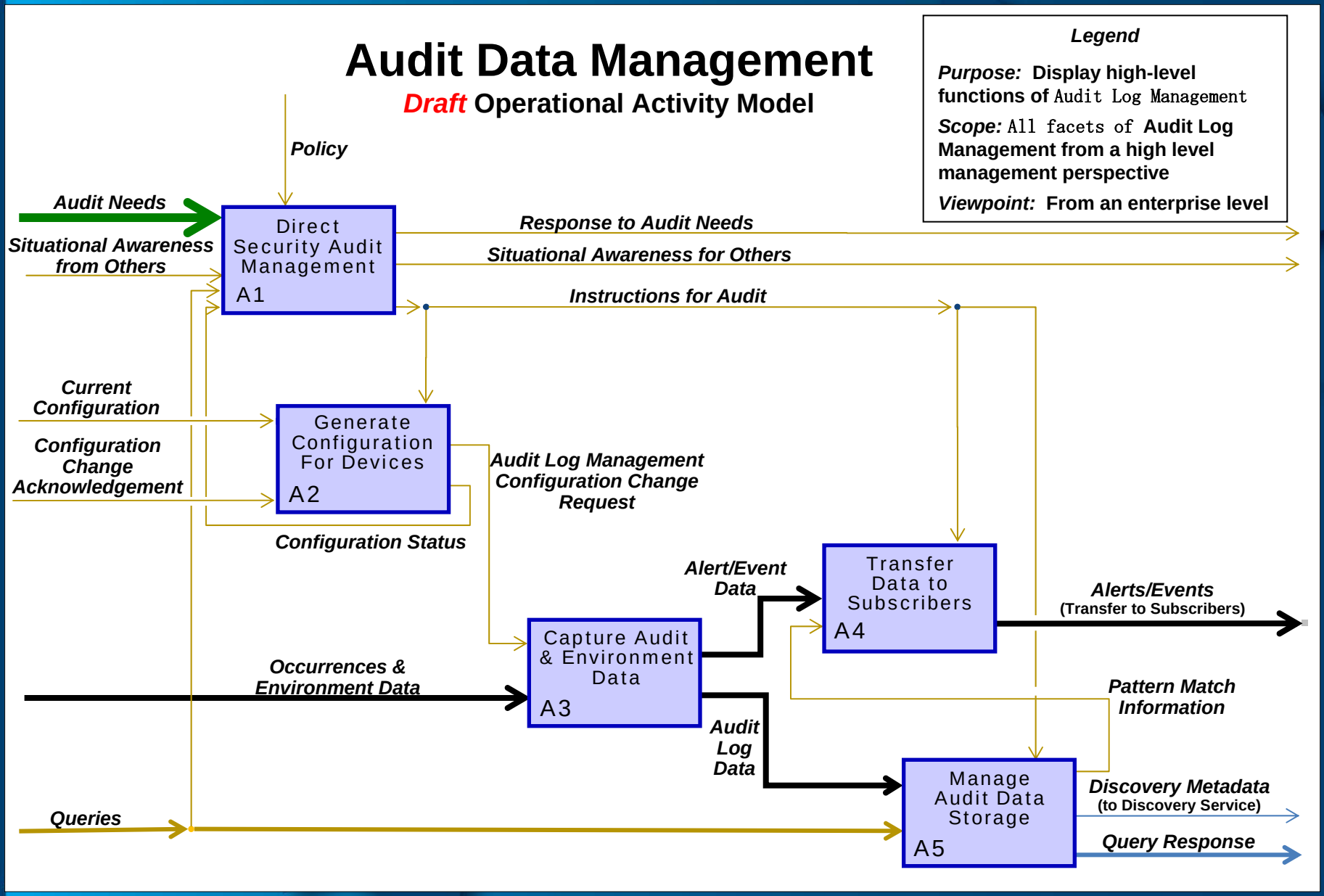
Capability Area	Capability Requirement Statements	Requirement Applicable To: Enterprise	CC/SIA	Regional	Local	Devices	Policy Issue to be Addressed	Source ("DEV"=Derived From
Normalization	(U) The ESM Audit Management function shall validate the syntactical correctness of audit log data.		•	•	•			DRV GIG IA Audit Management Gap Analysis Requirements spreadsheet (retrieved from ESM Portal)
Data Management	(U) The Regional level shall provide audit event log reduction to local and central repositories.			•				DRV GIG IA Audit Management Gap Analysis Requirements spreadsheet (retrieved from ESM Portal)
Normalization	(U) The CC/S/A audit functions shall convert audit event records in dissimilar formats into a common event language data representation.		•				Y	ESM Functional Decomposition
Data Management	(U) The CC/S/A audit functions shall combine low-level audit event records into a smaller number of higher level audit event records.		•					ESM Functional Decomposition
Analysis	(U) The Regional level audit function shall identify the type of audit event according to the common event categories enumerated in the common event language data			•				ESM Functional Decomposition

High-Level Architecture

- **Developing Operational and—*later*—Systems Architectures**
- **Building upon Functional Decomposition Audit Management from ESM Working Group**
- **Initial Top Level Operational Activity Model Drafted**
- **Ongoing Steps:**
  - Increased Detail for Operational Activity Model
  - Obtain Community Feedback
  - Refine Operational Architecture
  - ***Later***: System Architectures for Selected Design Alternatives

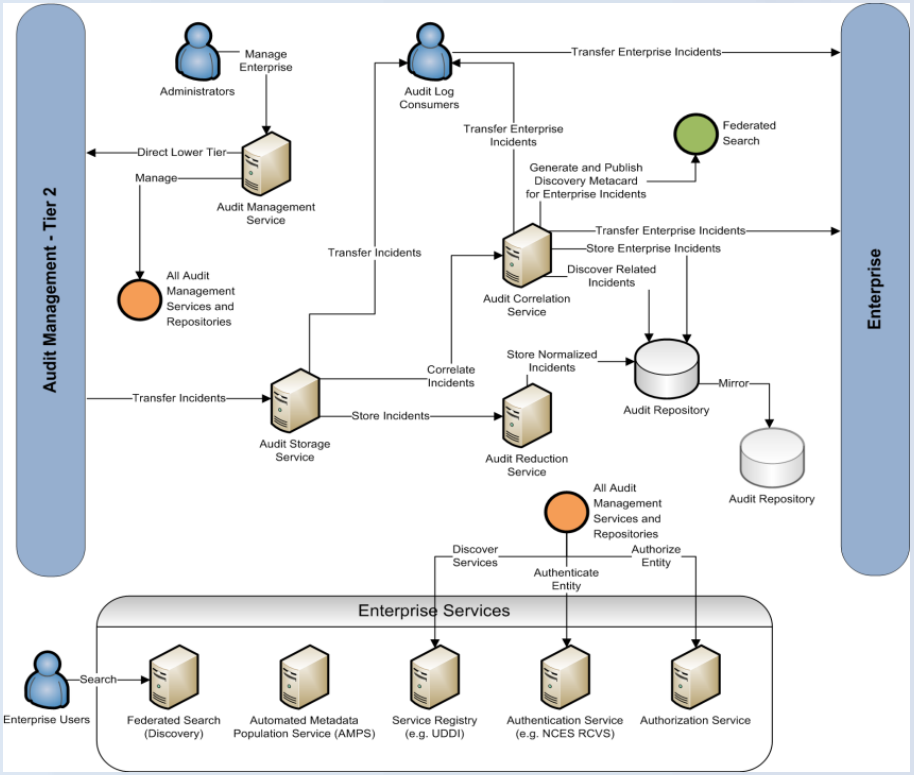


Top-Level Model of Enterprise-Wide Audit



High-Level Design of Enterprise Audit Components

- **Based on Requirements, Identifying "Trade Space" for Enterprise Audit Components**
  - Cost to Implement, Cost to Operate, Training, Bandwidth …
  - Store at Local Level vs Store at Enterprise Level …
- **Identifying Set of Alternative Designs for Audit Components**
  - Management & Direction
  - Storage
- **Upcoming Actions:**
  - Flesh out design alternatives
  - Solicit community feedback on trade-space & alternative designs.



Concept of Operations (CONOPS)

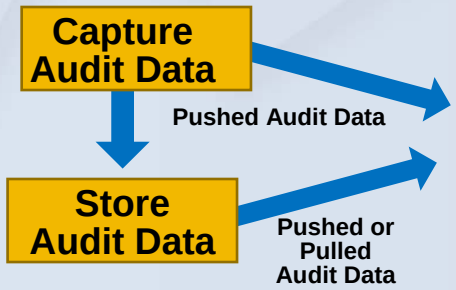
- **Explanations of *How to Use***
- **Addresses Non-Materiel Aspects**
  - Procedures
- **Anticipating a Family of CONOPS**
  - Separate CONOPS for distinct ***Roles***
  - Separate CONOPS same role at different ***Levels***
- **Upcoming Actions:**
  - As Audit Components are Designed, Prepare CONOPS for Applicable Roles & Levels

Examples of Likely CONOPS

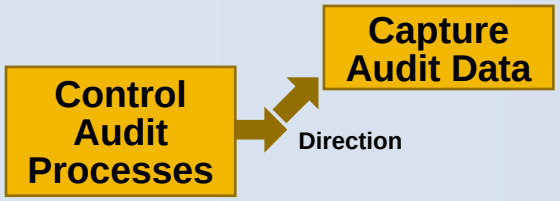
- Enterprise Audit Manager
- Service/Agency Audit Manager
- Audit Data Repository Manager – Tier-3
- Audit Data Repository Manager – Tier-2
- System Manager Audit Data Management
- LAN Administrator Audit Data Management

Schemas for Audit Data Management

- **Schema for Audit Data**
  - Common Event Expression (CEE)
  - Addresses:
    - Audit Events
    - Audit Records
    - Audit Logs
  - May be applicable to results of analysis of audit data.



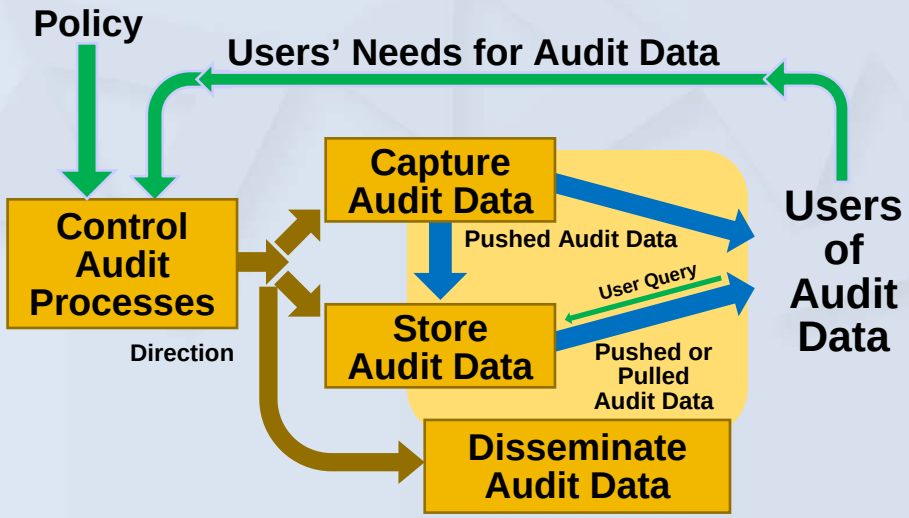
- **Schema for Directing Devices that Capture Audit Data**
  - Common Command Language

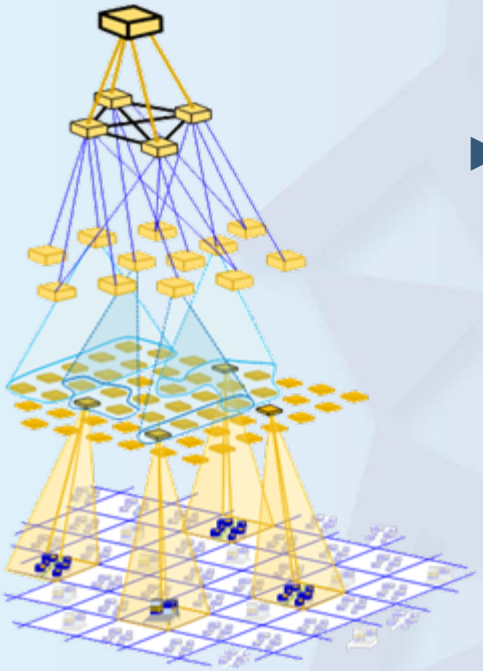


- **Other Schema …**

Enterprise-Wide Audit Data Management

- **Four Key Functions**
  - Capture Audit Data
  - Store Audit Data
  - Disseminate Audit Data
  - Control Audit Processes





- **Ongoing Efforts are Addressing:**
  - Requirements & Policy
  - Architectures & Design Alternatives
    - Variety of Trade Spaces
    - Allocation of Functions to Tiers of the Enterprise
  - Family of Concept of Operations
    - CONOPS by Role and Organizational Level
  - Schema for Standard Data Flows

Enterprise-Wide Audit-Data Management

Enterprise Security Management
Special Program Office (NSA/I5E)