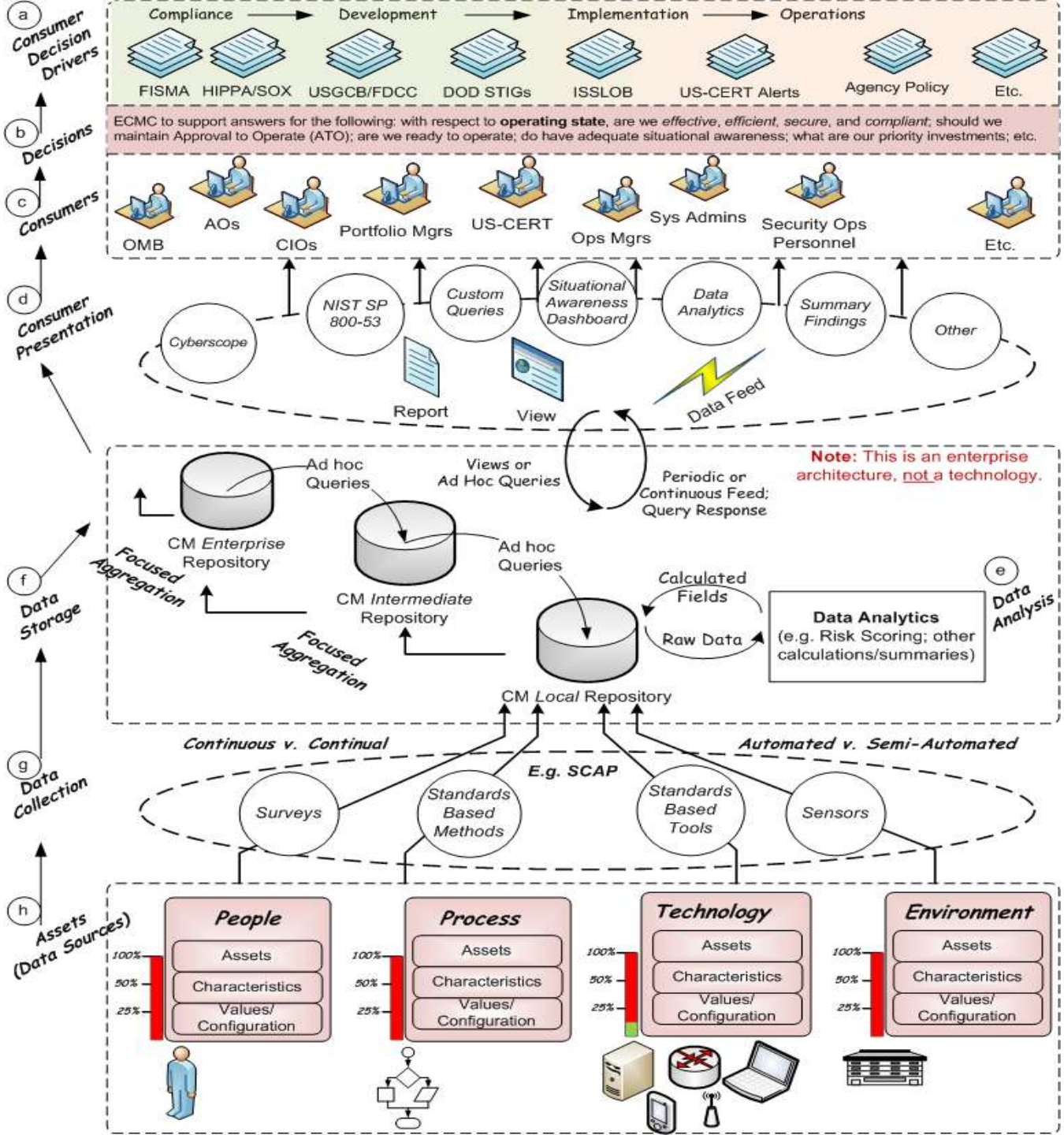

a
Consumer Decision Drivers
Compliance
Development
Implementation
Operations
FISMA
HIPPA/SOX
USGCB/FDCC
DOD STIGs
ISSLOB
US-CERT Alerts
Agency Policy
Etc.
b
Decisions
ECMC to support answers for the following: with respect to operating state, are we effective, efficient, secure, and compliant; should we maintain Approval to Operate (ATO); are we ready to operate; do have adequate situational awareness; what are our priority investments; etc.
c
Consumers
OMB
AOs
CIOs
Portfolio Mgrs
US-CERT
Ops Mgrs
Sys Admins
Security Ops Personnel
Etc.
d
Consumer Presentation
Cyberscope
NIST SP 800-53
Custom Queries
Situational Awareness Dashboard
Data Analytics
Summary Findings
Other
Report
View
Data Feed
Note: This is an enterprise architecture, not a technology.
Ad hoc Queries
Views or Ad Hoc Queries
Periodic or Continuous Feed; Query Response
CM Enterprise Repository
Ad hoc Queries
CM Intermediate Repository
Focused Aggregation
Focused Aggregation
f
Data Storage
Calculated Fields
Raw Data
Data Analytics
(e.g. Risk Scoring; other calculations/summaries)
e
Data Analysis
CM Local Repository
Continuous v. Continual
Automated v. Semi-Automated
E.g. SCAP
g
Data Collection
Surveys
Standards Based Methods
Standards Based Tools
Sensors
h
Assets (Data Sources)
People
Assets
Characteristics
Values/ Configuration
100%
50%
25%
Process
Assets
Characteristics
Values/ Configuration
Technology
Assets
Characteristics
Values/ Configuration
Environment
Assets
Characteristics
Values/ Configuration

CAESARS:
Continuous Asset Evaluation, Situational Awareness, and Risk Scoring - Reference Architecture

Homeland Security

Why CAESARS?

About 80% of known computer vulnerabilities are attributed to misconfiguration or missing patches.

Two basic approaches for keeping systems secure

- **Centralized:** Lock down workstation and server images, push patches as soon as available and tested
  - Works well only in tightly controlled environments
  - Risks introducing changes that break applications if not well tested
- **Decentralized:** Make users responsible for keeping systems patched
  - Works only if users cooperate and do their part
  - Risks leaving systems unpatched, misconfigured, vulnerable

CAESARS helps control the decentralized approach

- **Improves Asset Mgmt., Configuration Mgmt., Vulnerability Mgmt.**
- **Provides information tailored to decision makers at all levels**

Homeland Security

Key prerequisites for success

Clear Responsibility

- All managed assets are known, accessible, and assigned to someone for responsibility

Clear Standards

- Assets have an approved baseline of security configuration and patches

Knowledge: What to do

- Management and system owners have detailed, accurate, timely status information on every asset's configuration and patch status

Ability: How to do it

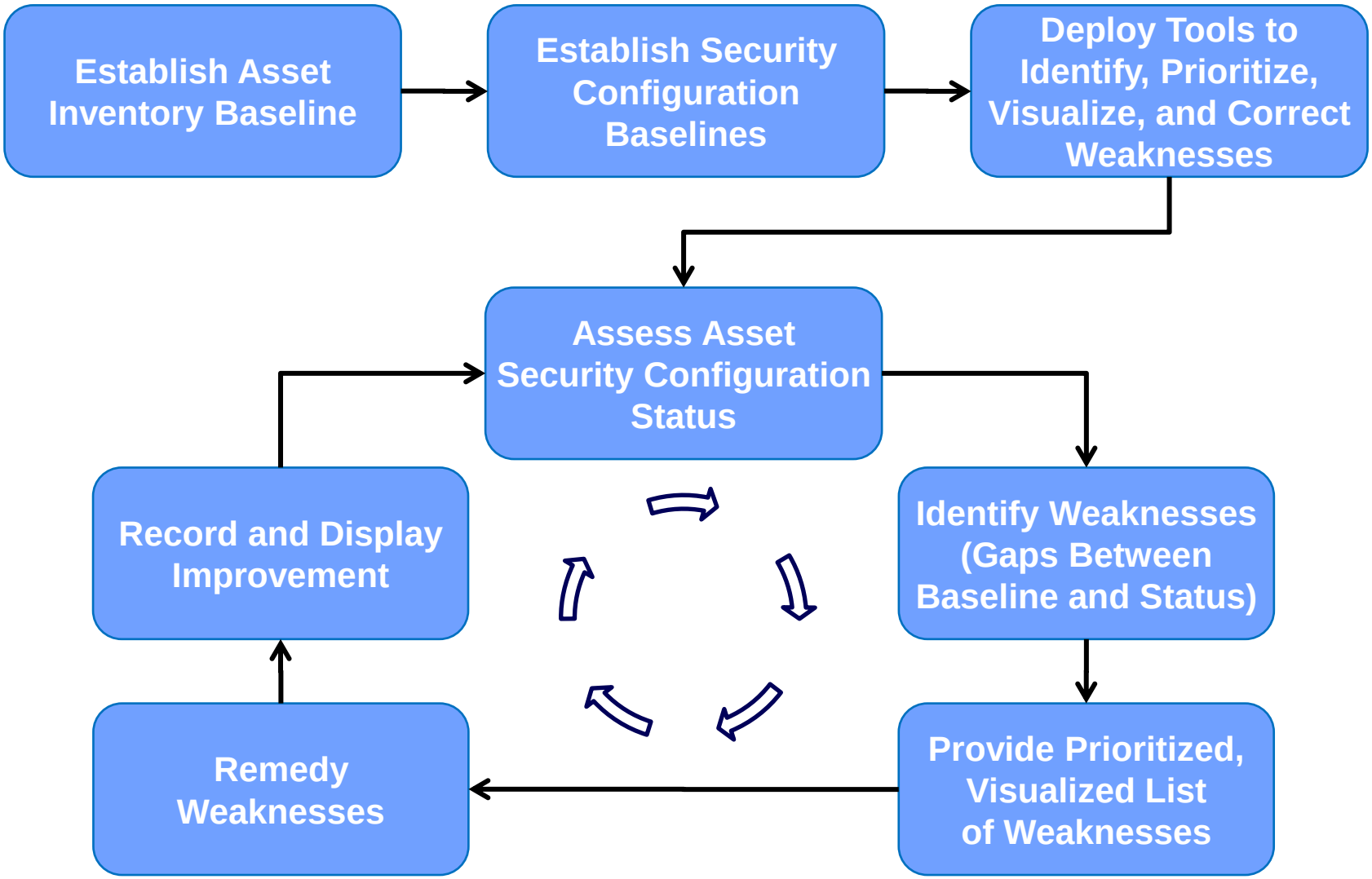
- System owners have a realistic opportunity to keep assigned assets in acceptable condition on a timely basis and the tools to control configuration of their assets

Motivation: Why to do it

- Dashboard reflects relative state of security health, enabling fair comparisons. Motivation must fit each organization's culture.

Homeland Security

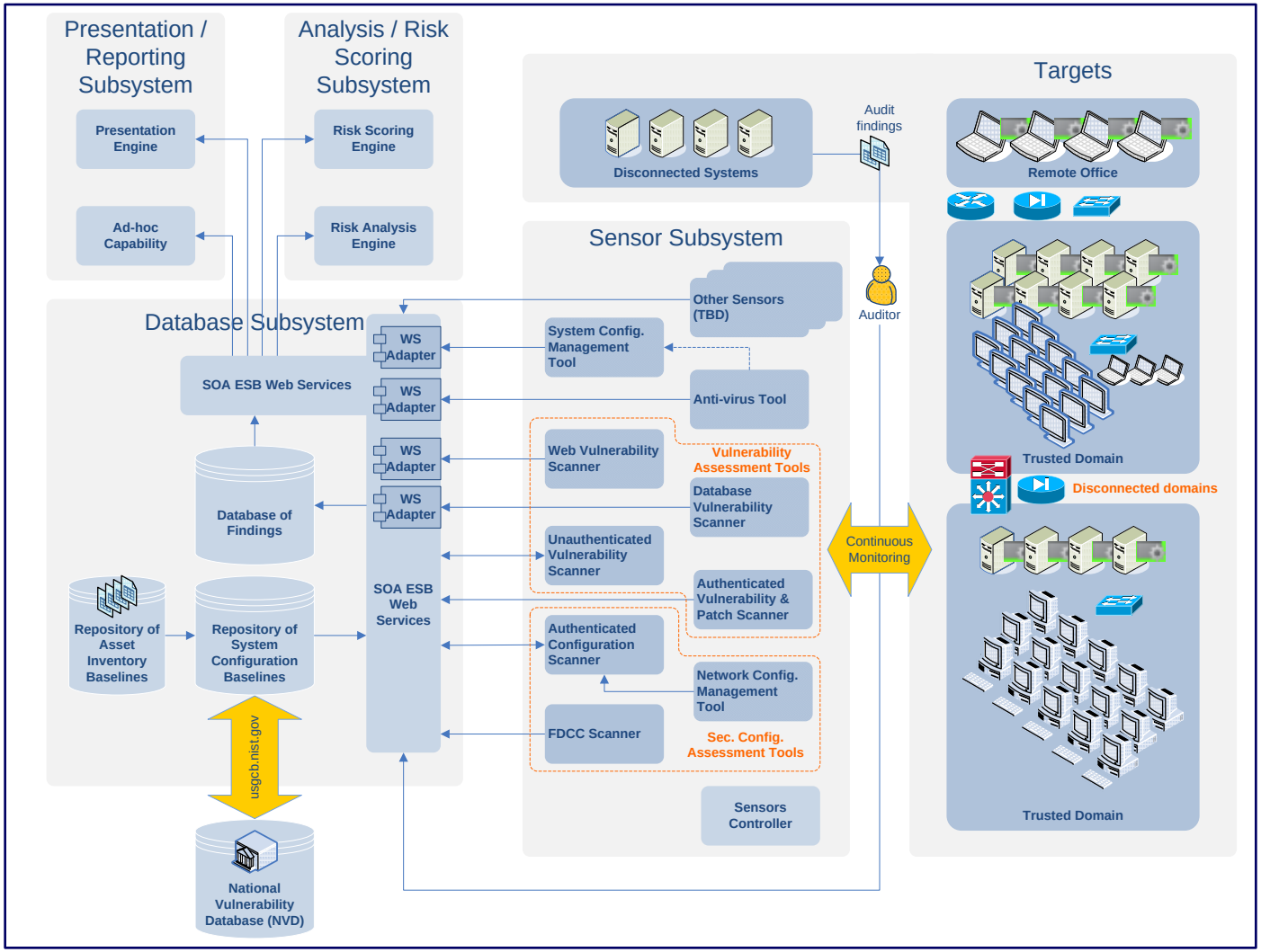
Risk Reduction Process Supported by Tools



Homeland Security

CAESARS* Reference Architecture:

*Continuous Asset Evaluation, Situational Awareness, and Risk Scoring



Homeland Security

Required System Capabilities

1. Continuously monitor and measure the effectiveness of implemented security controls
2. Manage security configuration throughout the system life cycle
3. Implement the standard protocols and technology – Security Content Automation Protocol (SCAP)
4. Automate to reduce level-of-effort in security operations
5. Facilitate management of information security risks
6. Support change control process and manage security configuration baseline

Homeland Security

Data Analysis versus Risk Scoring

Data Analysis is *interpretation-neutral* *(objective)*

- Any deviation from the acceptable/expected baseline is a weakness
- Original data is always available by drill-down, e.g., for remediation

Risk Scoring is *interpretation-specific* *(subjective)*

- Combining/reducing data, e.g., by weighting results, represents an Enterprise policy decision as to relative importance of weaknesses
- What is appropriate for one agency or environment may not be for another

Data Analysis and Risk Scoring are parallel but separate

- Both can be done off-line, particularly if time- or compute-intensive
- All users can always see interpretation-specific details
- Even at Enterprise level, original data is still available

Homeland Security

Caveats and Disclaimers

Risk scoring is not a substitute for other management and operational controls.

It can't determine which IT systems have the most *impact* on agency operations.

It can't determine how security failures will affect the *functions and mission of the organization.*

It is not a substitute for underlying governance and management processes that assign *responsibility and accountability* for agency processes and results.

Homeland Security

BACKUP

Homeland Security

Example Risk Scoring Algorithm Formulas

Score Component	Scoring Formula	Notes
Vulnerability Management	VUL Score = .01 * (CVSS Score)^3. Host VUL Score = SUM(VUL scores of all detected vulnerabilities)	To provide greater separation between HIGH and LOW vulnerabilities (so that it takes many LOWs to equal one HIGH vulnerability), the raw CVSS score is transformed by raising to the power of 3 and dividing by 100.
Patch Compliance	Host PAT Score = SUM(PAT scores of all incompletely installed patches)	**Patch Risk Level** / **Risk Score** Critical / 10.0 High / 9.0 Medium / 6.0
Security Compliance	Host SCM Score = SUM(SCM scores of all FAILed checks)	SCM Score for a failed check = Score of the check's Security Setting Category
Anti-Virus Compliance	Host AVR Score = (IF Signature File Age > 6 THEN 1 ELSE 0) * 6.0 * Signature File Age	After six days, a score of 6.0 is assigned for each day since the last update of the signature file, starting with a score of 42.0 on day 7.
Standard Operating Environment Compliance	Host SOE Score = SUM(SOE product scores)	Product SOE Score = 5.0 (for each product not in approved SOE version)
User Password Age	UPA Score = (IF PW Age > 60 THEN 1 ELSE 0) * 1.0 * (PW Age – 60)	Exceptions: The user account is disabled, or The user account requires two-factor authentication for login
Computer Password Age	CPA Score = (IF PW Age > 30 THEN 1 ELSE 0) * 1.0 * (PW Age – 30)	By means of Group Policy Objects, workstations should refresh passwords every 7 days; server refresh is set to 30 days.
SMS Reporting	Host SMS Score = (IF Error Code = 1xx/2xx THEN 1 ELSE 0) * (100.0 + 10.0 * (SMS Reporting Age))	Error codes have been added to SMS. An error code of 1xx or 2xx indicates unreliable reporting of Patch, Anti-Virus, and SOE status.
Vulnerability Reporting	Host VUR Score = (IF VUR Age > 15 THEN 1 ELSE 0) * 5.0 * FLOOR ((VUR Age - 15)/7	If a host has never been scanned, e.g., the host is new on the network, the current date is used as the base date.
Security Compliance Reporting	Host SCR Score = (IF SCR Age > 30 THEN 1 ELSE 0) * 5.0 * FLOOR ((SCR Age – 30) / 15)	If a host has never been scanned, e.g., the host is new on the network, the current date is used as the base date.

Homeland Security