How Were the CDM Capabilities Defined?

Organizations may define certain security capabilities needed to satisfy security requirements and provide appropriate mission and business protection. Security capabilities are typically defined by bringing together a specific set of safeguards/countermeasures (i.e., security controls) derived from the appropriately tailored baselines that together produce the needed capability.

NIST SP 800-53 Security Controls

Access Control
Awareness & Training
Audit & Accountability
Security Assessment & Authorization
Configuration Management
Contingency Planning
Identification and Authentication
Incident Response
Maintenance
Media Protection
Physical & Environmental Protection
Planning
Personnel Security
Risk Assessment
System & Services Acquisition
System & Communications Protection
System & Information Integrity

CDM Capabilities

Data Loss Prevention
Network Access Control
Respond to Incidents & Contingencies
Detect Suspicious Events / Patterns
Prepare for Incidents & Contingencies
Boundary Protection
Manage Privileges
Manage Credentials & Authentication
Manage Security Related Behavior
Manage Trust in People Granted Access
Vulnerabilities Management
Configuration Settings Management
Software Asset Management
Hardware Asset Management

Working with NIST, DHS distilled the SP 800-53 security controls into CDM (security) capabilities to provide D/As across the Federal Enterprise with a common baseline implementation of automated security controls assessment.

Individual controls are grouped by the desired results, helping to simplify the conceptual link between security controls and business results.

The complete set of CDM capabilities includes all SP 800-53 high-impact baseline security controls.