System Center Operations Manager 2007
Data Warehouse and ACS Database Reporting and Archiving

**ECC eSCOP Functional Challenge ...**

**eSCOP ACS COMPLIANCE REPORTING**

Over 250 Pre-Defined Reports through consolidated reporting dashboard console for Sarbanes Oxley, HIPAA, GLBA, PCI, FISMA and other regulatory compliance related auditing. Compliance reports are based on international standards (ISO, NIST, etc) into report families, report functional categories and individual event reports.

Over 22 data filtering management parameters, over 150 sub-parameters

- Begin Date Time
- End Date and Time
- Agent Computer
- Event Computer
- Source
- Category
• Header Sid
• Header User
• Header Domain
• Primary Sid
• Primary Domain
• Primary Logon ID
• Client Sid
• Client User
• Client Domain
• Target Sid
• Target User
• Target Domain
• Client Logon Id

REPRESENTATIVE LIST OF COMPLIANCE REPORTS

Multiple report types including standard, expanded forensic, complete (string data included), graphical pie and histogram comparisons and trend analysis
LIST OF COMPLIANCE RELATED REPORTS

Access Control – Family Reports Inclusive
Recommended IT security specifications define twenty access control sub-families. eSCOP provides auditing and reporting functions for key measurable controls supported by targeted Microsoft platforms.

Account Management – Functional Category Reports
The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts
User Account was created – Event Report
User Account type was changed – Event Report
User Account was enabled – Event Report
User Account password was changed – Event Report
User Account password was set – Event Report
User Account was disabled – Event Report
User Account was deleted – Event Report
General account database was changed – Event Report
User Account was changed – Event Report
User Account was locked – Event Report
Computer Account was created – Event Report
Computer Account was changed – Event Report
Computer Account was deleted – Event Report
Name of an account was changed – Event Report
Password Policy Checking API Called – Event Report

Account Enforcement – Functional Category Reports
The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.
Process is using an invalid located procedure call (LPC) port to impersonate a client and reply or read from or write to a client address space – Event Report
Access was granted to an already existing object – Event Report
Handle to an object was closed – Event Report
Attempt to open an object with the intent to delete it was made
A protect object was deleted – Event Report
Access was granted to an already existing object type – Event Report
A generic object operation took place – Event Report
Permission associated with a handled was used – Event Report
Attempt to create a hard link to a file being audited was made – Event Report
Resource Manager of Authorization Manager attempted to create a client context – Event Report
The client attempted to access an object – Event Report
The client context was deleted by the Authorization Manager – Event Report
Administrator Manager initialized the application – Event Report
Privilege Service Called – Event Report
Privileges were used on an already open handle to a protected object – Event Report
New Process was created – Event Report
Process Exit – Event Report
Object handle was duplicated – Event Report
Object was indirectly accessed – Event Report
Audible Data was protected – Event Report
Audible Data was unprotected – Event Report
Primary Token was assigned to an object – Event Report
User attempted to install a service – Event Report
Schedule job was created – Event Report
User right was assigned – Event Report
User right was removed – Event Report
System access was granted – Event Report
System access was removed – Event Report

**Information Flow Enforcement** – Functional Category Reports
The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

**Separation of Duties** – Functional Category Reports
Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).

Trust Relationship with another domain was created – Event Report
Trust Relationship with another domain was removed – Event Report
Trust Relationship with another domain is changed – Event Report
Global Group was created – Event Report
Global Group was created – Event Report
Global Group member was added – Event Report
Global Group member was removed – Event Report
Global Group was deleted – Event Report
Local Group was created – Event Report
Local Group member was added – Event Report
Local Group member was deleted – Event Report
Local group was deleted – Event Report
Local group account was changed – Event Report
Global Group was changed – Event Report
Domain Policy was changed – Event Report
Local Security Group with Security Disabled was Created – Event Report
Local Security Group with Security Disabled was Changed – Event Report
Local Security Group Member Added – Event Report
Security Disabled Local Group Member Removed – Event Report
Security disabled local group was deleted – Event Report
Security-disabled Global Group was created – Event Report
Security-disabled Global Group was changed – Event Report
Member of a Security-disabled Global Group was added – Event Report
Member of Global Security-disabled Group was removed – Event Report
Security-disable Global Group was deleted – Event Report
Universal Group was created – Event Report
Universal Group was changed – Event Report
Member of a Universal Group security-enabled was added – Event Report
Member of Universal Group security-enabled was removed – Event Report
Universal Group was deleted – Event Report
Universal Security-disabled group was created – Event Report
Universal Security-disabled group was changed – Event Report
Member of Universal Security-disabled group was added – Event Report
Member of Universal Security-disabled group was removed – Event Report
Member of Universal Security-disabled group was deleted – Event Report
Group type was changed – Event Report
Set the security redirector for administrative groups – Event Report
Trusted forest information was added – Event Report
Trusted forest information was deleted – Event Report
Trusted forest information was modified – Event Report
Role separation enabled – Event Report

**Least Privilege** – Functional Category Reports

The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Global Group member was added – Event Report
Global Group member was removed – Event Report
Local Security Group Member Added – Event Report
Member of a Security-disabled Global Group was added – Event Report
Member of Global Security-disabled Group was removed – Event Report
Member of a Universal Group security-enabled was added – Event Report
Member of Universal Group security-enabled was removed – Event Report
Member of Universal Security-disabled group was added – Event Report
Member of Universal Security-disabled group was removed – Event Report
Member of Universal Security-disabled group was deleted – Event Report
Local Security Group Member Deleted – Event Report

**Unsuccessful Login Attempts** – Functional Category Reports

The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded. Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Logon to disabled account failed – Event Report
Logon to expired account failed – Event Report
Logon by non-allowed type failed – Event Report
Logon due to expired password failed – Event Report
Logon failed due to inactive logon service – Event Report
Logon for other reasons failed – Event Report
Logon during account lock-out failed – Event Report
Logon failure due to SID difference with trusted domain and account domain – Event Report
Logon from untrusted forest namespace failed – Event Report
Logon by unauthorized computer user failed – Event Report

**Session Termination** – Functional Category Reports
The information system automatically terminates a session after [Assignment: organization-defined time period] of inactivity.

User reconnected to a disconnected terminal server connection – Event Report
User disconnected terminal services connection without logging off – Event Report

**Remote Access** – Functional Category Reports
The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

User reconnected to a disconnected terminal server connection – Event Report
User disconnected terminal services connection without logging off – Event Report

**Audit and Accountability** – Family Reports Inclusive
The audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required.

**Content and Auditing Reporting** – Functional Category Reports
The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

Auditing policy was set on a per-user basis – Event Report
Per User Audit Policy was changed – Event Report
Audit policy was changed – Event Report
Event log service read the security log configuration for a session – Event Report

**Audit Storage Capacity** – Functional Category Reports
The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

Audit Log was exhausted – Event Report
Event Log was cleared – Event Report
Security log auditing failed – Event Report
Audit Log Capacity – Event Report

**Audit Processing** – Functional Category Reports
In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)].
Audit Log was exhausted – Event Report
Event Log was cleared – Event Report
Security log auditing failed – Event Report
Audit Log Capacity – Event Report
Audit Collection failed – Event Report

Audit Monitoring, Analysis and Reporting – Functional Category Reports
The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
Audit policy was changed – Event Report
Event log service read the security log configuration for a session – Event Report

Time Stamps – Functional Category Reports
The information system provides time stamps for use in audit record generation. Time stamps of audit records are generated using internal system clocks that are synchronized system wide.
The system time was change – Event Report

Identification and Authentication – Family Reports Inclusive
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

User Identification and Authentication – Functional Category Reports
The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.
Logon was successful – Event Report
Logon failure from unknown user name or bad password – Event Report
Logon failed by user outside allocated time – Event Report
Logon to disabled account failed – Event Report
Logon to expired account failed – Event Report
Logon by non-allowed type failed – Event Report
Logon due to expired password failed – Event Report
Logon failed due to inactive logon service – Event Report
Logon for other reasons failed – Event Report
Logoff by user was completed – Event Report
Logon during account lock-out failed – Event Report
Logon to network was successful – Event Report
Logon failure due to SID difference with trusted domain and account domain – Event Report
Logon from untrusted forest namespace failed – Event Report
User log off process was initiated – Event Report
User logon with explicit credentials while logged on as different user – Event Report
Authentication Service (AS) ticket was issued and validate – Event Report
Ticket Granting Service (TGS) ticket was issued – Event Report
Security Principal was renewed as AS or TGS Ticket – Event Report
Preauthorization failed – Event Report
Authorization ticket failed – Event Report
TGS ticket was not granted – Event Report
An account was successfully mapped to a domain account – Event Report
NTLM Successfully Authenticates User – Event Report
NTLM failed when login attempt to domain – Event Report

**Device Identification and Authentication** – Functional Category Reports
The information system identifies and authenticates specific devices before establishing a connection. The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.

Logon by unauthorized computer user failed – Event Report
Main Mode IKE Connection to peer was complete – Event Report
Data channel was terminated – Event Report
Main mode was terminated – Event Report
Main mode failed due to peer invalid certificate or signature – Event Report
Main mode failed due to Kerberos failure or invalid password – Event Report
IKE security establishment failed due to invalid peer proposal – Event Report
IKE handshake failed – Event Report

**Identifier Management** – Functional Category Reports
The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers. Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts).

User Account was created – Event Report
User Account type was changed – Event Report
User Account was enabled – Event Report
User Account password was changed – Event Report
User Account password was set – Event Report
User Account was disabled – Event Report
User Account was deleted – Event Report
General account database was changed – Event Report
User Account was changed – Event Report
User Account was locked – Event Report
Computer Account was created – Event Report
Computer Account was changed – Event Report
Computer Account was deleted – Event Report
Name of an account was changed – Event Report
Password Policy Checking API Called – Event Report

**Authenticator Management** – Family Reports Inclusive
The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.
Authentication package was located by the Local Security Agent (LSA) – Event Report
Trusted Logon Process was registered by the Local Security Agent – Event Report
Notification package was loaded on the Security Accounts Manager – Event Report
IPSec Policy was changed – Event Report
IPSec Policy agent encountered a potentially serious failure – Event Report
Kerberos policy was changed – Event Report
Encrypted Data Policy was changed – Event Report
Certificate Manager denied a pending certificate request – Event Report
Certificate Services received a resubmitted certificate request – Event Report
Certificate Services revoked a certificate – Event Report
Certificate Services received a request to publish the certificated revocation list (CRL) – Event Report
Certificate Services publish the CRL – Event Report
A certificate request extension was made – Event Report
One or more certificate request attributes changed – Event Report
The security permissions for Certificate Services changed – Event Report
Certificate Services retrieved an archival file – Event Report
Certificate Services imported a certificate into the database – Event Report
The audit filter for Certificate Services changed – Event Report
Certificate Services received a certificate request – Event Report
Certificate Services approved a certificate request – Event Report
Certificate Services denied a certificate request – Event Report
Certificate Services set the status of a certificate request to pending – Event Report
The certificate manager settings for Certificate Services change – Event Report
A Configuration entry changed in Certificate Services – Event Report
A property of Certification Services change – Event Report
One or more rows have been deleted from certificate database – Event Report

**System and Communication Protection – Family Reports Inclusive**
The organization develops, disseminates, and periodically reviews/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance

**Application Partitioning** – Functional Category Reports
The information system separates user functionality (including user interface services) from information system management functionality. The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

**Denial of Service Protection** – Functional Category Reports
The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].

Notification of possible denial of service attack was sent – Event Report

**Transmission Integrity** – Functional Category Reports
The information system protects the integrity of transmitted information.

Quality of Service Policy Changed – Event Report
Encrypted Data Policy was changed – Event Report
Main Mode IKE Connection to peer was complete – Event Report
Data channel was terminated – Event Report
Main mode was terminated – Event Report
Main mode failed due to peer invalid certificate or signature – Event Report
Main mode failed due to Kerberos failure or invalid password – Event Report
IKE security establishment failed due to invalid peer proposal – Event Report
IKE handshake failed – Event Report

Transmission Confidentiality – Functional Category Reports
The information system protects the confidentiality of transmitted information.

Main Mode IKE Connection to peer was complete – Event Report
Data channel was terminated – Event Report
Main mode was terminated – Event Report
Main mode failed due to peer invalid certificate or signature – Event Report
Main mode failed due to Kerberos failure or invalid password – Event Report
IKE security establishment failed due to invalid peer proposal – Event Report
IKE handshake failed – Event Report

Network Disconnect – Functional Category Reports
The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.

Data channel was terminated – Event Report
User disconnected terminal services without logging off – Event Report

Cryptographic Key Establishment – Functional Category Reports
The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

IPSec Policy was changed – Event Report
Kerberos policy was changed – Event Report
Encrypted Data Policy was changed – Event Report
Certificate Manager denied a pending certificate request – Event Report
Certificate Services received a resubmitted certificate request – Event Report
Certificate Services revoked a certificate – Event Report
Certificate Services received a request to publish the certificated revocation list (CRL) – Event Report
Certificate Services publish the CRL – Event Report
Certificate Services import a certificate into the database – Event Report
Certificate Services received a certificate request – Event Report
Certificate Services approved a certificate request – Event Report
Certificate Services denied a certificate request – Event Report
Certificate Services set the status of a certificate request to pending – Event Report
Certificate Services changed the certificate manager settings for Certificate Services change – Event Report
A Configuration entry changed in Certificate Services – Event Report
A property of Certification Services changed – Event Report
System and Information Integrity – Family Reports Inclusive
The information system verifies the correct operation of security functions

Security Verification Functions – Functional Category Reports
The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.

- Server Startup – Event Report
- Server Shutdown – Event Report
- IPSec Policy Agent was started – Event Report
- IPSec Policy Agent was disabled – Event Report
- Certificate Services received a request to shutdown – Event Report
- Certificate Services restore started – Event Report
- Certificate Services started – Event Report

Contingency Planning – Family Reports Inclusive
The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and stores backup information at an appropriately secured location.

Information System Backup – Functional Category Reports
The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and stores backup information at an appropriately secured location. The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization’s recovery time objectives and recovery point objectives.

- Data Protection Master Key was backed up – Event Report
- Data Protection Master Key was recovered from a recovery server – Event Report
- Certificate Services backup started – Event Report
- Certificate Services archived a log – Event Report
- Certificate Services imported and archived a key – Event Report
- Certification services published the certificate authority (CA) certificate to AD – Event Report

Information Recovery and Reconstruction – Functional Category Reports
The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system’s original state after a disruption or failure. Secure information system recovery and reconstitution to the system’s original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.

- Data Protection Master Key was backed up – Event Report
- Data Protection Master Key was recovered from a recovery server – Event Report
- Certificate Services backup started – Event Report
Certificate Services restore completed – Event Report
Certificate Services archived a log
Certificate Services imported and archived a key
Certification services published the certificate authority (CA) certificate to AD