

Federal Information Security Management Act  
Enterprise Compliance Auditing & Reporting

***ECAR™ for FISMA***

Technical Product Overview Whitepaper

**ECAR™ for FISMA Product Abstract**

Federal Information Security Management Act (FISMA) impacts governmental agencies and commercial contracting organizations. FISMA requires compliance with an exhaustive number of technical, operational and management requirements. The National Institute of Science and Technology's (NIST) Special Publication 800-53 provides recommended guidance for FISMA compliance.

The ECC Enterprise Compliance Auditing and Reporting (ECAR) system maps over 175 Microsoft Windows IT security events to the technical and operational specifications defined by NIST SP 800-53. Utilizing Microsoft Operations Manager (MOM) server, events are tracked and a variety of auditing reports are generated.

**ECAR™ FISMA FEATURES**

Over 175 Windows Server IT Security Events  
Collective and Individual Event Views  
Audit Reports and Trails  
Fully Customizable and Extensible  
Events mapped to NIST FISMA Recommended Controls:  
*Access Control Management*  
*Audit and Accountability*  
*Contingency Planning*  
*Identification and Authentication*  
*System and Information Integrity*  
*System and Communication Protection*

# ECC Enterprise Compliance Auditing and Reporting (ECAR) Federal Information Security Management Act (FISMA) Windows IT Security Controls Using Microsoft Operations Manager

## INTRODUCTION

The Federal Information Security Management Act (FISMA) was enacted to protect critical data infrastructures and promote best practice standards. The National Institute of Science and Technology (NIST) assumed responsibility for interpreting the legislation and translating the goals into understandable and achievable guidelines. As it relates to FISMA, NIST Special Publication 800-53 seeks to assist government agencies and commercial contracting organizations to understand and achieve compliance. [NIST SP 800-59 and related documents identifies issues impacting national security systems.]

Failure to comply with FISMA may result in very significant administrative sanctions on agencies and government contractors. Beyond punitive actions, the NIST FISMA recommendations should be regarded as positive IT security guidance. In developing ECAR, Enterprise Certified Corporation embraced the baseline NIST recommendations as solidly grounded and consistent with international IT security best practice standards.

A major challenge for IT professionals is to measure FISMA compliance with repeatable audits and processes to produce meaningful and accurate reports. The Microsoft Windows server platform provides information on individual security events generated as accounts access electronic information and perform activities that can be manually reviewed via log files. However, this process is time consuming and ad hoc. The ECC Enterprise Compliance Auditing and Reporting (ECAR) solution for FISMA maps over 175 Microsoft Windows security events to key technical and operational NIST SP800-53 guidelines. ECAR leverages information gathered and organized using Microsoft Operations Manager (MOM) monitoring and event collection capabilities. The IT administrator can examine these events from a

variety of views and output reports based on such criteria as time periods, computer groups, users, domains and event IDs.

## BACKGROUND: SECURITY CONTROLS

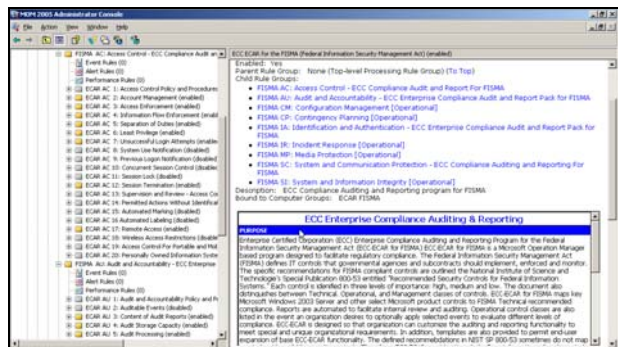
The selection and employment of appropriate *security controls* for an information system is fundamental. NIST breaks down security controls into three safeguard families: management, operational, and technical. The purpose is to protect the confidentiality, integrity, and availability of systems and information. While certain NIST FISMA guidelines are procedural, many of the technical and operational recommendations are IT event driven and lend themselves to ECAR's automated compliance auditing and reporting.

ECAR is designed to assist organizations subject to FISMA to collect and report on Microsoft Windows server platform IT events. The goal is to facilitate a more consistent, comparable, and repeatable approach that is consistent with recommended minimum security controls for information systems as categorized by Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Through the use of the MOM infrastructure, ECAR promotes a dynamic, extensible catalog of security controls for information systems.

## WHO BENEFITS FROM ECAR

ECAR is intended to serve a diverse federal audience of information system and security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and

project managers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit.



ECCAR FOR FISMA ADMINISTRATIVE CONSOLE

### SECURITY CONTROL BASELINES

Organizations must employ security controls to meet security requirements defined by laws, executive orders, directives, policies, or regulations (e.g., Federal Information Security Management Act, OMB Circular A-130, Appendix III).<sup>15</sup> The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would comply with the stated security requirements. Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task.

### TAILORING THE INITIAL BASELINE

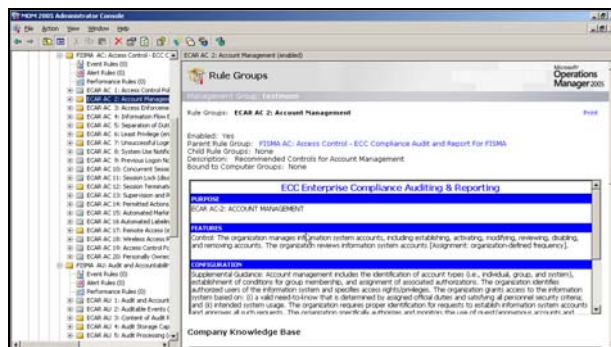
After the appropriate security controls are selected, three additional steps are needed to tailor the baseline for a specific organizational information system: (i) the application of *scoping guidance* to the initial baseline; (ii) the specification of *organization-defined parameters* in the security controls, where appropriate; and (iii) the specification of *compensating security controls*, if needed. By default, ECC ECAR provides the initial framework, reports, and regulatory knowledge.

However, organizational fine tuning will still be required. To ensure a cost-effective, risk-based approach to achieving adequate information security organization-wide, tailoring activities should be coordinated with appropriate officials (e.g., senior agency information security officers, authorizing officials). The resulting set of security controls should be documented in the security plan for the information system and integrated with the ECAR system.

### REVISIONS AND EXTENSIONS

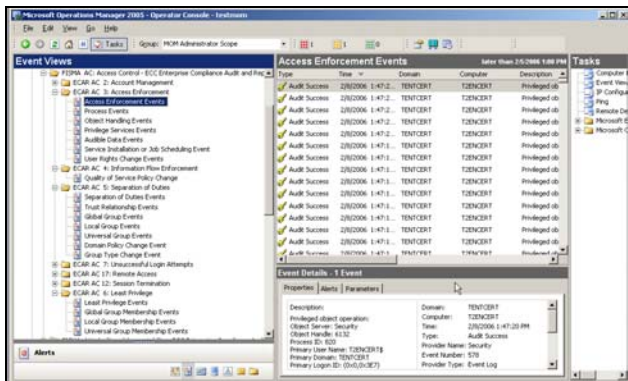
The set of security controls listed in the control catalog and the ECAR associated Windows server platform IT events represents a baseline of safeguards and countermeasures for information systems. ECAR is designed to facilitate revision and extensions to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within organizations; and (iii) new security technologies that may be available. The events and controls populating the various families will change over time, as operating systems and applications are added and updated. ECAR is designed to also accommodate governmental regulatory additions, deletions, or modifications to the catalog of security controls.

NIST has defined minimum security controls as having the low, moderate, and high baseline levels of impact. It is anticipated that these will also change over time as well. Therefore, ECAR permits the movement of IT security events between the recommended controls. ECAR, together with MOM, facilitates dynamic and flexible technical auditing and reporting of a rigorous set of security controls in a cost-effective manner.



ECCAR FISMA/NIST SOURCED KNOWLEDGE BASE

Security controls containing configurable parameters give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, directives, executive orders, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. ECAR permits organizations to map IT security events to a variety of views in order to facilitate granular and targeted security audits.



ECAR EVENT VIEWS

## ECAR SUPPORTED SECURITY CONTROLS

By default, ECAR supports the following NIST SP800-53 security controls. The ECAR infrastructure also allows the user to add, delete and modify the default events that are associated with other recommended controls.

### FAMILY: ACCESS CONTROL

#### CLASS: TECHNICAL

**AC-2 ACCOUNT MANAGEMENT** - The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

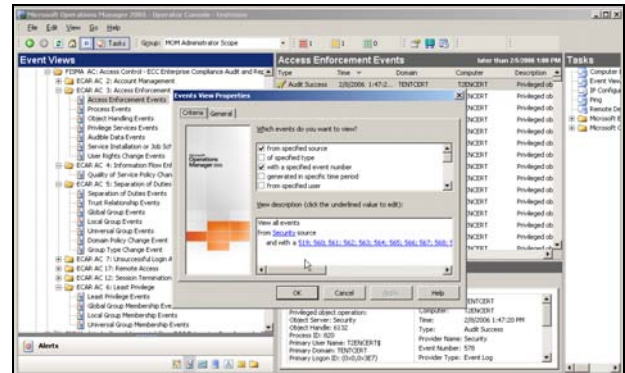
**AC-3 ACCESS ENFORCEMENT** - The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

**AC-4 INFORMATION FLOW ENFORCEMENT** - The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

**AC-5 SEPARATION OF DUTIES** - The organization establishes appropriate divisions of responsibility and

separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

**AC-6 LEAST PRIVILEGE** - 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.



ECAR/MOM Custom Event Views

**AC-7 UNSUCCESSFUL LOGIN ATTEMPTS** - The information system enforces a limit on consecutive invalid access attempts by a user during a time period.

**AC-12 SESSION TERMINATION** - The information system automatically terminates a session.

**AC-17 REMOTE ACCESS** - 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.

### FAMILY: AUDIT AND ACCOUNTABILITY

#### CLASS: TECHNICAL

**AU-3 CONTENT OF AUDIT RECORDS** - 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.

**AU-4 AUDIT STORAGE CAPACITY** - The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

**AU-5 AUDIT PROCESSING** - 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

**AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING** - 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.

**AU-8 TIME STAMPS** - The information system provides time stamps for use in audit record generation.



ECAR Default Reports

**FAMILY: CONTINGENCY PLANNING**  
**CLASS: OPERATIONAL**

**CP-9 INFORMATION SYSTEM BACKUP** - 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.

**CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION** - 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.

**FAMILY: IDENTIFICATION AND AUTHENTICATION**  
**CLASS: TECHNICAL**

**IA-2 USER IDENTIFICATION AND AUTHENTICATION** - The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

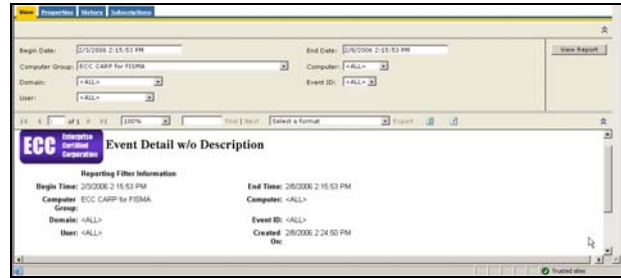
**IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION** - The information system identifies and authenticates specific devices before establishing a connection.

**IA-4 IDENTIFIER MANAGEMENT** - 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.

**IA-5 AUTHENTICATOR MANAGEMENT** - 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.

**IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION** -For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.



ECAR REPORT SAMPLE

**FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION**  
**CLASS: TECHNICAL**

**SC-2 APPLICATION PARTITIONING** - The information system separates user functionality (including user interface services) from information system management functionality.

**SC-3 SECURITY FUNCTION ISOLATION** - The information system isolates security functions from non-security functions.

**SC-5 DENIAL OF SERVICE PROTECTION** - The information system protects against or limits the effects of the following types of denial of service attacks.

**SC-8 TRANSMISSION INTEGRITY** - The information system protects the integrity of transmitted information

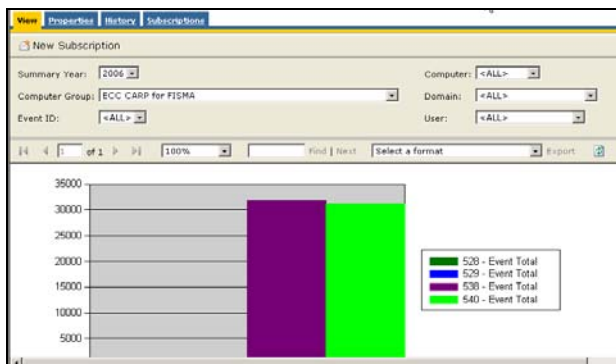
**SC-9 TRANSMISSION CONFIDENTIALITY** - The information system protects the confidentiality of transmitted information.

**SC-10 NETWORK DISCONNECT** - The information system terminates a network connection at the end of a session or after inactivity

**SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT** - The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

**FAMILY: SYSTEM AND INFORMATION INTEGRITY**  
**CLASS: OPERATIONAL**

**SI-6 SECURITY FUNCTIONALITY VERIFICATION** - The information system verifies the correct operation of security functions): *upon system startup and restart.*



ECAR Sample Graphical Report

### ECAR, MICROSOFT AND NIST

The Microsoft Windows Server platform provides IT professionals about 200 security events that can be used for regulatory compliance auditing and reporting. The Microsoft Operation Manager facilitates the collection of events and manages the ability to customize views and reports. Building on this foundation ECC developed ECAR around NIST recommendations as a compliance auditing and reporting environment. ECAR is used to identify security compliance issues for both assessment and mitigation purposes. As the proactive monitoring capability of the MOM platform progresses, so will an organization's ability to react and adjust its risk posture. ECAR provides the framework to achieve these ends.

ECC wants to acknowledge the ground breaking efforts of NIST and in particular the team responsible for SP 800-53.

#### SYSTEM REQUIREMENTS:

- Microsoft Windows 2003 Server
- Microsoft Operations Manager
- SQL Server with Reporting Services
- Trademarks of Microsoft Corporation



#### ABOUT ECC

Enterprise Certified Corporation is the developer and publisher of risk management solutions focused on IT security regulatory compliance. The firm is comprised of world-class IT security and Windows experts including the authors of best selling books like the *Ultimate Windows 2003 Server System Administrator's Guide*. In addition, Microsoft has honored principals with four Most Value Professional awards in the field of Windows Security. The company participates in many industry organizations such as the Sarbanes Oxley executive roundtable and the Department of Homeland Security/FBI's Infragard.

For more information about ECC and its other solutions go to:

<http://www.enterprisecertified.com>

1-800-701-2785 Sales Ext. 4 Service Ext. 5

ECAR™ is a trademark of Enterprise Certified Corporation ALL RIGHTS RESERVED WORLD WIDE

**ECC Enterprise Compliance Auditing and Reporting (ECAR)**  
**Federal Information Security Management Act (FISMA)**  
**Windows IT Security Controls Using Microsoft Operations Manager**