

## Enterprise Compliance Auditing and Reporting

ECC Enterprise Compliance Auditing and Reporting (eCAR™) aligns over 175 Microsoft® Windows IT security events with specific regulatory requirements and best standards recommendations. Easily customized and extensible, IT-related security data is gathered and organized in a fashion that is immediately useable for IT professional response, internal management review and external examination. Over 100 reports are mapped directly to individual regulations and may be output to a large number of file/archive formats. Leveraging Microsoft's System Center Operations Center 2007 and Auditing Collection Service, the eCAR™ IT security solution provides audit and reporting information focused on the growing regulatory demands of Sarbanes Oxley, FISMA, HIPAA, GLBA, PCI and others.



### ECAR™ Solution for Today

ECC ECAR™ is designed to facilitate the audit process associated with IT security event assessment and regulatory compliance auditing/reporting.

Recognizing that many organizations must address multiple regulatory requirement, eCAR™ Plus provides a crosswalk approach to event management and reporting. Alternatively, customers can select a version for individual regulations such as the Federal Information Security Management Act (FISMA), Gramm Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes Oxley Act. Each version ties directly to the expectations associated with the individual legislative and associated agency initiatives. Events are tracked in the following category families:

- Access Control
- Audit and Accountability
- Contingency Planning & Management
- Identification and Authentication
- System and Communications Protection
- System Information Integrity

Knowledgebase support for specific auditing and reporting functions is associated with best standards such as those from the National Institute of Science and Technology (NIST), COSO, ISO 17799, and the Federal Financial Institutions Examination Council (FFIEC).

### Key Benefits

ECC ECAR™ unique mapping of IT security events to regulations and standards streamlines the assessment process and provides greater assurance of producing meaningful audits and reports. The unified approach is sustainable, repeatable and measurable. The web-based report generator provides the administrator to set parameters and IT events that are most applicable for security assessment and regulatory auditing of a particular organization. Utilizing the infrastructure afforded Microsoft System Center Operations Manager and SQL Server 2005 Reporting Services, ECC ECAR™ provides regulatory aligned rules groups and definable event views.

**On demand, continuous and customized analysis** – ECC ECAR™ automatically collects IT security information for predefined events, rules and computer group associations that have a direct relation to a regulation or standard. This activity remains continuous for all enabled functions. In addition, special reports can be output based upon very granular administrator defined on-demand requirements. Whether standard or customized configuration is desired, audit integrity is maintained so longevity and “slice of time” information is readily available.

When Risk Management and Control Is Critical ...

# ECC ECAR™ Enterprise Compliance Auditing & Reporting

**Centralized and inherently useful information** – ECC ECAR™ was designed to provide IT security event information that would be useful for a variety of user audiences. IT administration is provided a variety of levels of formatted data that permit summary and in depth analysis. Columnar, group and graphical reports make review by non-technical management something that is viable and readily available. For external auditors or government examination teams, IT security events are assembled in a fashion that maps to their regulatory inspection guidelines. Where disputes should occur, the alignment of ECC ECAR™ to best practice standards provides greater justification for current and proposed policies and procedures. All is centralized and secure.

**Intuitively Useful Reporting**– ECC eECAR™ ships with 100 customizable management reports built around security and compliance requirements. The multiple format reports provides summary, detailed, and forensic expanded reports. Graphical report output includes event comparisons,

occurrence percentages and trend analysis. The enhanced ECC caching technology accelerates reporting on even millions of event records.

## Alternative SCOM Data Warehouse or ACS Storage

Two versions of eCAR are available to support either the standard System Center Operations Manager 2007 data warehouse database or the optional Audit Collection Service (ACS).

When implementing the SCOM 2007 version, user will be collecting and reporting against the default database schema. This option reduces some administration and added resource requirements.

Alternatively, for organizations that want to assure greater audit trial integrity, then the ACS version is recommended. In essence, ACS collects security events in a separate database in order to promote greater audit integrity. The eCAR™ ACS module adds functional control, logical archiving, compliance oriented viewing, and management reporting.

## Other Features

**Out of the Box Compliance Oriented Rules, Views and Reports:** The eCAR™ arranges events into recognized families including Access Management, Audit Management, Contingency Planning, Identification and Authentication, and System and Network Management.

**Integrated Knowledge Base:** ECC eCAR™ provides extensive integrated knowledge base on IT security events, industry best practice standards, and individual regulatory requirements.

**Cross Platform and Localized Options:** Working in association with industry partners, ECC can optionally extend event collection and analysis to other operating systems and network devices.

**Expert Based:** ECC eCAR™ is designed and supported by award winner IT security and compliance experts.



**For Additional Information:**  
[www.enterprise-certified.com](http://www.enterprise-certified.com)  
[eSCOP@enterprise-certified.com](mailto:eSCOP@enterprise-certified.com)  
 800 701 2785 ext 4

The screenshot displays the ECC ECAR software interface. On the left is a navigation tree with categories like 'AC: Access Control', 'AU: Audit and Accountability', and 'IA: Identification and Authentication'. The main area is divided into several panes:

- Filter Information:** Shows search criteria for 'March, 2007' with date pickers for 'Begin Time' (3/10/2007) and 'End Time' (3/21/2007). It includes dropdowns for 'Agent Computer', 'Event Computer', 'Header User', 'Primary User', 'Client User', and 'Target User'.
- Event Detail Table:** A table with columns 'Event ID', 'Creation Time', and 'Agent Computer'. It lists several events with IDs like 538, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553.
- Percentage Graph:** A pie chart showing the distribution of event counts across different categories.
- Bar Chart:** A bar chart showing event counts for different categories.
- Event Description Window:** A pop-up window titled 'EventDescription' showing details for Event ID 529. It includes fields for 'Agent Computer', 'Event Computer', 'Category', 'Source', 'Header', 'Primary', 'Client', and 'Target'. The description text reads: 'Logon Failure: Reason: Unknown user... SE\_AUDITID\_UNKNOWN\_USER\_D...'. It also shows 'Logon Type: 10', 'Source Network Address: 192.168.0.10', 'Source Port: 3574', 'Workstation Name: ECAREVAL', 'Caller Process ID: 2760', and 'Transited Services: -'. An explanation at the bottom states: 'This event record indicates an attempt to log on using an unknown user account or a valid user account but with an incorrect password. An unexpected present an attempt by someone to "dictionary" attack, in which a list of'.

