Netsurion | EventTracker

ISO 27002: 2013 Audit Standard Solution Brief

www.netsurion.com/eventtracker

ISO 27002

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.

Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

ISO 27002:2013 Audit Standards

ISO 27002 began life as the Information Security 'Code of Practice' from the UK's Department of Trade and Industry.

ISO 27002, Code of Practice for Information Security, is a commonly used international standard for information security throughout the world and provides insight to security controls to protect information and information technology. ISO 27002 does not address how to apply the controls. ISO 27001 provides direction on how to establish a management system that superimposes a discipline over how to select controls and how to establish good practices to apply the security controls. The procedures, to actually implement the security controls are up to the organization and will vary according to the physical and technical environment.

To establish an appropriate code of practice for information security management in alignment with the ISO 27002 standard, many security controls across IT infrastructure must be implemented. For compliance to Communications and Operations Management and Information Security Incident Management, data throughout the network systems, applications and databases must be monitored and analyzed. For doing it affordably and reliably, the right automated security solution is required that offers end-to-end data correlation, in-depth analysis and detailed reporting to ISO 27002 compliance mandates.

ISO 27002 regulations established by the International Organization for Standardization provide best-practice recommendations on information security management. Importantly, ISO 27002 controls, offer guidance for those who are responsible for initiating, implementing, and maintaining Information Security management systems (ISMS), in an effort to:

- Prevent unauthorized users from gaining access to business systems and confidential company data.
- Safeguard the accuracy and completeness of information and processing methods.
- Ensure that authorized users have necessary access to information and associated assets.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker SIEM improves security, helps organizations demonstrate compliance, and increases operational efficiencies. EventTracker SIEM enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

SIEMphonic is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, ISO 27002 audit reports annotation, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker SIEM provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security and ISO 27002 standard.

EventTracker SIEM provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMWAre ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker SIEM is available on premise or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

ISO27002:2013 Audit Standard

ISO27002:2013 Audit Standard	EventTracker Solution	EventTracker Reports	EventTracker Alerts
A.12.4.1 Event logging Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. Event logs should include, when relevant: • User IDs • System Activities • Dates, times and details of key events, e.g. log-on and log-off • Device identity or location if possible and system identifier • Records of successful and rejected system access attempts • Records of successful and rejected data and other resource access attempts • Changes to system configuration • Use of Privileges • Use of system utilities and applications • Files accessed and the kind of access • Network addresses and protocols • Alarms raised by the access control system • Activation and de-activation of protection systems, such as anti-virus systems and intrusion Detection systems • Records of transactions executed by users in applications Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.	Monitoring system use requires organizations to accurately manage user access rights. It addresses the issues of unintended or malicious modifications of information assets. Deficiencies in this area may allow unauthorized modifications that could lead to errors in reporting. User access rights to systems and data should be in line with defined and documented business needs and job requirements. Organizations must monitor and verify all user access to programs and data, and review this access to ensure that all access privileges are properly assigned and approved. In addition, all logins to network devices, operating systems/platforms, databases and applications must be reviewed to ensure only authorized and appropriate personnel have access. To satisfy this control objective, administrators must periodically review the user access to files and programs to ensure the users have not accessed items outside of their role. Administrators should select a sample of users who have logged in to reporting servers and review their access for appropriateness based upon their job functions. Administrators should also set up real-time alerts to detect any unauthorized or unapproved changes to users or groups. Monitor account management activities such as user or group addition /deletion / modification to ensure all user access privileges are appropriate and approved. Once the event logging is enabled, EventTracker is capable of collecting and storing the events. Thus, the user can easily monitor any activity and generate alerts and reports, as required.	Yes	Yes
A.12.4.2 Protection of log information Logging facilities and log information should be protected against tampering and unauthorized access. Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including: • Alterations to the message types that are recorded • Log files being edited or deleted • Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events. Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence. System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security *(continued)*	A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Administrators must ensure that IT security implementation is tested and monitored proactively. IT security should be reaccredited periodically to ensure that the approved security level is maintained. Access to the logging information is in line with business requirements in terms of access rights and retention requirements. IT security administration must monitor log security activity, and identify security violations to report to senior management. This control directly addresses the issues of timely detection and correction of data modification. To satisfy this requirement, administrators must review the user access logs on a regular basis or on a weekly basis for any access violations or unusual activity. Administrators must periodically, such as daily or weekly, review reports that show user access to servers related to the ISO process. Review of these reports must be shown to auditors to satisfy this requirement. *(continued)*	Yes	Yes

ISO27002:2013 Audit Standard	EventTracker Solution	EventTracker Reports	EventTracker Alerts
A.12.4.2 Protection of log information (continued) monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered. System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.	In addition, administrators must ensure that all relevant log sources are logging properly to a centralized log management system. EventTracker's solution is developed from a ground up to be a regulatory compliance solution. All log messages can be transferred via TCP to ensure reliability. All the received logs will be archived. EventTracker performs a checksum on the cab files and monitors the changes or modification done on the same. It is also capable of generating reports and alerts in case the data is tampered.		
A.12.4.3 Administrator and operator logs System administrator and system operator activities should be logged and the logs protected and regularly reviewed. Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users. An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.	All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. Administrators and root users should never directly access system components, as these accounts are generally shared and difficult to track back to a specific individual. Instead, these users should be accessing these components using commands such as sudo or su; or in the Window environment, assigned to an administrative group. This setup allows individuals' actions to be tracked. To satisfy this requirement, administrators must ensure all logins are not shared. Administrators must review the ID list to identify IDs that may be a generic ID and question who is using it and why it is there. EventTracker is capable of collecting and storing the events, once the event logging is enabled. Activities can be tracked and alerts, reports can be generated and viewed by the user.	Yes	Yes
A.16.1.7 Collection of evidence The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action. In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off. The procedures should take account of: • Chain of custody • Safety of evidence • Safety of personnel • Roles and responsibilities of personnel involved • Competency of personnel • Documentation • Briefing *(continued)*	Managing problems and incidents addresses how an organization identifies documents and responds to events that fall outside of normal operations. Organizations must maintain a complete and accurate audit trail for network devices, servers and applications, This enables organizations to address how business identify root causes of issues that may introduce inaccuracy in reporting. Also, problem management system must provide for adequate audit trail facilities that allow tracing from incident to underlying cause. Monitor any account management activities such as user or group addition/deletion/ modification to ensure all user access privileges are appropriate and approved. Set up real-time alerts to detect any unauthorized or unapproved changes to users or groups. Audit trails related to user creation and deletion of system-level objects, for example, a file, folder, registry key, printer, and others, are critical in the troubleshooting and forensic analysis processes. To satisfy this control objective, administrators must ensure all network devices, servers, and applications are properly configured to send logs to a centralized server. Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly. *(continued)*	Yes	Yes

ISO27002:2013 Audit Standard	EventTracker Solution	EventTracker Reports	EventTracker Alerts
A.16.1.7 Collection of evidence (continued) Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence. Forensic evidence may transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions. Identification is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence. Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence. When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required. ISO/IEC 27037 provides guidelines for identification, collection, acquisition and preservation of digital evidence.	Record at least the following audit trail entries for each event, for all system components: • Use of identification and authentication mechanisms • Creation and deletion of system-level objects. • Record at least the following audit trail entries for each event, for all system components: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource • Retain audit trail history for a period that is consistent with its effective use, as well as legal regulations. EventTracker allows the user to perform a historical log search based on the information required. Thus, the user can easily access any data required.		
A.9.4.1 Information access restriction Access to information and application system functions should be restricted in accordance with the access control policy. Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy. The following should be considered in order to support access restriction requirements: • Providing menus to control access to application system functions • Controlling which data can be accessed by a particular user • Controlling the access rights of users, e.g. read, write, delete and execute • Controlling the access rights of other applications • Limiting the information contained in outputs Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.	User access rights to systems and data should be in line with defined and documented business needs and job requirements. Accurately managing user access rights addresses the issues of unintended or malicious modifications of data. Deficiencies in this area may allow unauthorized modifications that could lead to errors in reporting. To satisfy this control objective, administrators must periodically review the user access to files and programs to ensure the users have not accessed items outside of their role. Administrators should select a sample of users who have logged in to reporting servers and review their access for appropriateness based upon their job functions. Administrators must monitor and verify all user access to programs and data. Review this access to ensure there is segregation of duties as well as all access privileges are properly assigned and approved. EventTracker is capable of collecting the events from various systems in a centralized location, and offers any access to information held in shares or applications, which can be monitored. Alerts and reports can also be generated for analysis purpose. For this, the auditing must be enabled on the resources.	Yes	Yes

ISO27002:2013 Audit Standard	EventTracker Solution	EventTracker Reports	EventTracker Alerts
A.12.7.1 Information systems audit controls Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes. • The following guidelines should be observed: Audit requirements for access to systems and data should be agreed with appropriate management • The scope of technical audit tests should be agreed and controlled • Audit tests should be limited to read-only access to software and data • Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements • Requirements for special or additional processing should be identified and agreed • Audit tests that could affect system availability should be run outside business hours All access should be monitored and logged to produce a reference trail.	Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. The auditor can obtain valuable information about activity on a computer system from the audit trail. Audit trails improve the auditability of the computer system. Organizations must maintain a complete and accurate audit trail for network devices, servers and applications. This enables organizations to address how businesses identify root causes of issues that may introduce inaccuracy in reporting. Also, problem management system must provide for adequate audit trail facilities that allow tracing from incident to underlying cause. IT security administration must monitor and log security activity, and identify security violations to report to senior management. This control directly addresses the control for audit controls over information systems and networks. To satisfy this control objective, administrators must ensure all network devices, servers, and applications are properly configured to log to a centralized server. Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly.	Yes	Yes
A.18.2.2 Compliance with security policies and standards Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review. If any non-compliance is found as a result of the review, managers should: • Identify the causes of the non-compliance • Evaluate the need for actions to achieve compliance • Implement appropriate corrective action • Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses. Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews when an independent review takes place in the area of their responsibility.	EventTracker allows the manager to view and analyze reports in the Top Level Summary option.	Yes	Yes

ISO27002:2013 Audit Standard	EventTracker Solution	EventTracker Reports	EventTracker Alerts
A.18.1.3 Protection of records Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. When deciding upon protection of specific organizational records, their corresponding classification based on the organization's classification scheme, should be considered. Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be stored to enable decryption of the records for the length of time the records are retained. Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturers' recommendations. Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change. Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled. The system of storage and handling should ensure identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization. To meet these record safeguarding objectives, the following steps should be taken within an organization: • Guidelines should be issued on the retention, storage, handling and disposal of records and information • A retention schedule should be drawn up identifying records and the period of time for which they should be retained • An inventory of sources of key information should be maintained Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure defense against potential civil or criminal action or to confirm the financial status of an organization to shareholders, external parties and auditors. National law or regulation may set the time period and data content for information retention.	EventTracker has the capacity to hold data and the System is also capable of writing and archiving the same in the configured path for storing purpose.	Yes	Yes