



Reports measuring the application of Metacontrols as they apply to the Sarbanes-Oxley Act.

*Intellitactics simplifies reporting with hundreds of packaged reports classified by regulatory standards (SOX, GLB, HIPAA, PCI and FISMA for the public sector). No other security information and event management solution offers a more complete catalogue of audit-worthy reports that provide evidence of compliance with standards. The following list of reports can be automatically generated and scheduled for distribution. Using the Report Wizard, you can edit any of these reports to create new reports, or you can write new reports using easy-to-follow templates. In addition, a report repository saves reports and tracks when reports are received. The compliance reports are available with Intellitactics Security Manager and Intellitactics for Compliance.*

### **Access Control**

Metacontrols which serve to limit and monitor the activities of users.

### **Account Management**

The organization manages all aspects of user account management including additions, deletions, modifications, lockouts, suspensions, activations and privilege changes.

Account Additions	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management	This report shows Security Manager user creation and deletion events for a specified time period.
Windows Account Creations	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes	This report shows the deletion of Windows accounts, audited by Windows event 630, sorted from the most recent to the oldest.
Windows Account Disables	This report shows the disabling of Windows accounts, audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to

	the oldest.
Windows Account Unlocked	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most recent to the oldest.

### Least Privilege

The organization should ensure that users are provided with the most minimal set of privileges required to carry out their designated duties in order to minimize the risk to organizational assets and business objectives. This mechanism shall include periodic reviews of privilege to identify users with excess privileges.

Group Changes	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
Security Manager Group Management	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.

### Monitor Login Activity

The organization should monitor all login activities to critical systems to ensure that data confidentiality and data integrity policies are followed.

Insecure Login Activity Alerts	This report shows alerts of the given type for a specified time period.
Top Accounts Failing Authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Successfully Authenticated Accounts	This report shows the most frequently observed accounts that authenticate successfully.
Windows Account Lockouts	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.
Windows Failed Logins	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.

### Network Access Control

Access to assets and their connected assets should be restricted to only those assets and accounts with a need to access network services and network protocols in order to further a business process or goal.

Top Firewall Denied Sources	This report shows the most frequently blocked source addresses.
Top Source Ports	This report shows the most frequently observed source ports.
Top Source Zones	This report shows the most frequently observed source address zones.
Top Sources	This report shows the most frequently observed source addresses.
Top Target Ports	This report shows the most frequently observed target ports.

Top Target Zones	This report shows the most frequently observed target address zones.
Top Targets	This report shows the most frequently observed target addresses.

### Remote Access Control

Organizations should have an authorization and approval process in place to control the granting of remote access to ensure that only the privileges required for carrying out assigned tasks and are provided via remote access. Additionally All remote access should be regularly monitored to ensure conformity with remote access policies.

Critical Asset Accessed Remotely Alerts	This report shows alerts of the given type for a specified time period.
VPN Account Login Summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity	This report shows denied attempts to log into VPN services.
VPN Login Activity	This report shows VPN login activity of a given user for a specified time period.

### Session Control

Information processing systems should be configured to automatically require re-authentication after a configurable period of time or inactivity.

Session Expiry for Privileged Account Alerts	This report shows alerts of the given type for a specified time period.
--	---

### Use of Non-Repudiation

The organization should employ non-repudiation methods for critical systems in order to irrevocably assign responsibility for system actions to a given individual or account.

Non-Repudiation Exception Alerts	This report shows alerts of the given type for a specified time period.
----------------------------------	---

### Wireless Access Control

The use of wireless technologies used to connect to information processing systems should be monitored closely to account for the additional risks as compared to other access control technical methods. Strong methods of authentication including physical access control, encryption, and multiple factor authentication.

Unauthorized WiFi WAP Summary	This report shows unauthorized WiFi access points.
WiFi Denied Auth Activity	This report shows denied attempts to authenticate for access to WiFi services.

### Business Continuity

Metacontrols which ensure that business continues in the face of unplanned events.

## Alternate Communications, Systems and Storage

The organization should provide alternate or redundant communications, systems and storage for information systems that are deemed vital to its continuity. These systems should be identified as part of a business continuity risk assessment.

Assets Unavailable	This report shows all events for a specified time period, where an asset has been shut down, restarted, or has encountered an error condition that has caused it to become unavailable.
Failover/HA Events	This report shows all events related to failover and high availability activities, including errors and other activities reported by devices, for a specified time period. This expands the scope of entries returned above the 'All Failover/HA Occurrences' report. These events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.
Failover/HA Occurrences	This report shows all failover and high availability events noted by Security Manager for a specified time period. Such events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.

## Software and Data Backup

Organizations must maintain recent and complete backup copies of software and data required for business continuity. These back-ups will be periodically validated to ensure they can be used to restore information processing systems to a current (data) and working (software) state.

Backup Service Activity	This report shows all activity related to backup services for a specified time period.
Security Manager SDW Backup	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.

## Certification - Accreditation - Compliance

Metacontrols ensuring compliance with regulations and fulfillment of the requirements of relevant certifications and accreditations.

## Continuous Monitoring of Controls

Organizations must continuously monitor controls to ensure adequate control coverage and acceptable control performance.

Registered Control Alerts	This report shows the registered control alerts for a specified time period.
Registered Control Reports	This report shows the registered control reports.
Report Requests	This report shows all Reporting System reports requested by an account for a specified time period.

Security Manager Activity	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account	This report shows all Security Manager activity by user account for a specified time period.

### Communications and System Protection

Metacontrols ensuring the protection of communication channels and the systems that use them.

#### Acceptable Use of Systems and Services

Organizations should have clear policies procedures regarding acceptable usage of systems & services. Monitoring should be performed to ensure that violations are detected and remediated.

Abuse by Account	This report shows all abuse-related events against the entered account for a specified time period.
Abuse by Asset	This report shows all abuse-related events for an entered source asset IP address over a specified time period. If a source asset IP address is not entered, results are grouped by the source asset IP address, regardless of whether or not it is a registered asset.
Top Web Referrals with Suspicious Responses	This report lists the URLs of pages referring to pages which, when requested, produce unusual HTTP response codes (307, 400, 401, 402, 405, 406, 408, 409, 410 through 419 and all 500 series).

### Mobile Code Protection

Organizations should create and enforce a policy on the proper use of mobile code in their information systems and networks.

Blocked Active Content to Critical Asset Alerts	This report shows alerts of the given type for a specified time period.
---	---

### Use of Cryptography

The organization should employ cryptographic techniques to aid in lowering risks to information processing systems and assets of disclosure and alteration.

VPN Errors	This report shows all VPN errors reported for a specified time period.
------------	--

### Voice over IP Security

Organizations should control the use of VOIP technology to ensure that availability of communications infrastructure is not impacted and to ensure that communications to and from the organization are always visible.

VOIP Service Activity	This report shows all activity related to VOIP services for a specified time period.
-----------------------	--

## Incident Response Management

Metacontrols ensuring that incidents are resolved in a thorough, timely and cost effective manner.

### Incident Handling

The organization should follow preestablished policies and procedures to prepare for, detect, analyze, contain, eliminate and recover from security incidents.

All Incidents	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Status	This report shows all incidents at each status for a specified time period.
Incidents by Close Date	This report shows the incidents closed for a specified time period.
Incidents by Create Date	This report shows the incidents created for a specified time period.
Open Incidents	This report shows all open incidents sorted from oldest to most recent for a specified time period.

### Incident Reporting

The organization should ensure that all necessary stakeholders are informed of incidents and that incidents are escalated as required by their risks. Escalation and notification processes should be well defined and automated whenever possible.

Incident Summary by Closing User	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

## Operations Management

Metacontrols which ensure that the organization's operations are carried out in a secure fashion.

### Asset Management

Organizations should classify information system assets by defining security categories that are based on established risk levels. This security categorization should be based on a risk assessment that takes into account the asset's value and the costs associated with the potential loss to the organization should controls fail to protect the asset.

Asset Additions	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a

	value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

### Capacity Management

Resource allocation and usage should be monitored, reviewed and adjusted with a view to forecasted future capacity requirements. Systems should be optimized for efficiency and increased capacity.

Average Count of Events per Day	This report shows the average number of events per day over a given period of time.
Average Count of Managed Events per Day	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.
Count of Events by Day	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.
Count of Managed Events by Day	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.
Resource Allocation Errors	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

### Monitoring Audit Logs

Organizations should continuously monitor all audit logs to ensure that both information systems and the privileges provided to users on those systems are consistent with normal business usage.

Acquired Devices	This report shows hosts from which ISM acquired events within the specified time period.
Unparsed Event Summary	This report shows devices for which some events could not be parsed.
Untaxonomized Events	This report shows Event ID values without taxonomy types from events within the specified time period.

### Monitoring Configuration Activity

Organizations should continuously monitor all configuration changes to information processing systems. This process includes verifying that users are authorized to make changes to an asset and the changes made are consistent with established policies and practices for that asset.

Configuration Activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

## Monitoring System Faults

System errors and faults should be monitored to identify assets that require intervention to maintain acceptable integrity and availability.

Critical Asset Error Alerts	This report shows alerts of the given type for a specified time period.
Errors	This report shows all errors reported for a specified time period.
Hosts with Errors Summary	This report shows hosts reporting errors within a specified time period.
Resource Allocation Errors	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

## Monitoring Use of Privileges

The organizations should monitor the activities of administrative users and the use of administrative privileges and utilities to ensure usage consistent with business policies and business needs.

SU/SUDO Use	This report shows all use of SU and SUDO tools for a specified time period.
-------------	---

## Physical and Environmental Security

Metacontrols which ensure that the physical information technology environment is secure.

### Physical Access Control

Organization should protect all means of gaining physical entry to it's facilities adequately by employing detective and preventive measures such keypad locks, electronic card readers, guards and cameras.

Physical Access Denied	This report shows all denied attempts to access secured areas/rooms for a specified time period.
------------------------	--

## Risk Assessment

Metacontrols which ensure that the organization measures risks to make informed security decisions.

### Assessment of Risk

Organizations must periodically employ risk assessment mechanisms that take into account factors such as: threats, vulnerabilities, assets, operational risk and business priorities. This ensures that all decisions regarding policies, controls and incidents are made with a full understanding of the potential cost or benefit to the organization.

High Risk Alerts	This report shows high risk alerts for a specified time period.
High Risk Alerts Involving Accounts	This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a

	specified time period.
High Risk Alerts on Critical Assets	This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater than or equal to the entered value for a specified time period.

### **Vulnerability Assessment**

The organization should maintain continuous awareness of newly discovered technical vulnerabilities that affect its information systems and rapidly assess and mitigate the risks as appropriate.

Asset Vulnerabilities	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

### **System Acquisition - Development - Maintenance**

Metacontrols ensuring that systems are acquired, developed and maintained to meet defined requirements and do so in a secure way.

### **Use of System Maintenance Tools**

Organizations should monitor the tools and utilities used for system maintenance to ensure they are not used to circumvent privileges levels and restrictions.

New Executable Loaded on Critical Asset Alerts	This report shows alerts of the given type for a specified time period.
--	---

### **System and Data Integrity**

Metacontrols to ensure that system and information changes are made in a planned, controlled and audited manner.

#### **Data Integrity Monitoring**

The organization should monitor information systems for changes to system software, applications & application data to detect unauthorized or irregular changes to data that could put the organization at risk with its customers, employees and partners.

Database Schema Changes	This report shows all events where a database schema change has occurred, for a specified time period. Compare these results to organizational change requests to identify unauthorized changes. This report is also useful when troubleshooting database driven application errors.
Monitored File Changes on Critical Asset Alerts	This report shows alerts of the given type for a specified time period.

### **Electronic Messaging Security**

The organization should monitor the security of all electronic messaging platforms to ensure the confidentiality, integrity and availability of all messages originating from or destined to the organization and its stakeholders.

Authentication to Email Failures	This report shows events where an account has failed to authenticate to electronic messaging services (Email only).
Blocked Electronic Messages	This report shows events that specify that an electronic message was not delivered. The reasons for message delivery failure will be indicated in the result set and will be attributed to one of the following conditions: 1. A firewall blocked the message from delivery due to a policy employed on the firewall. 2. Antivirus software interfered with message delivery. 3. A message was redirected to another delivery point (such as spam). 4. A message was partially modified by content filters (such as spam and antivirus prior to being delivered).

### **Intrusion Detection and Protection**

The organization should employ technologies and procedures monitor and protect all information systems from unwanted or unauthorized access attempts.

IDS/IPS Alerts	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures	This report shows the most frequently blocked IPS signatures.

Top Host IDS Event Types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types	This report shows the most frequently occurring event types.
Top Network IDS Event Types	This report shows the most frequently occurring event types.

### Malicious Code Protection

The organization should take adequate measures to protect it's IT infrastructure against malicious code such as viruses, worms and trojans by employing protective technologies on its networks and information systems.

Hosts with Most Malware Types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as the 'Types/Host' column.
Top Malware Types	This report shows the most frequently observed malware types.

*Thank you for your interest in the Intellitactics compliance and control reports. The reports are categorized into 11 groups including each of the standards, controls and management report types to make them easier to review. Also included are six sample reports representative of different report types. These are static lists of reports offered in the Intellitactics products. Updated versions of the list are always available through your Intellitactics Sales Representative.*

**To Contact Intellitactics:** 1800 Alexander Bell Drive. Suite 500. Reston, VA 20191  
[salesinfo@intellitactics.com](mailto:salesinfo@intellitactics.com) or 877-746-7658

