

# BASEL II Compliance

BASEL II, or the International Convergence of Capital Measurement and Capital Standards, represents recommendations by European Economic Union bank supervisors and central bankers to align capital reserves with levels of credit risk and operational risk. Designed to encourage greater uniformity in the way banks and banking regulators approach risk management internationally, the core tenets – or “pillars” – of compliance include: requirements, review, and discipline. Reporting on the security profile of the financial institution is a significant factor of BASEL II.

## Objectives to Meet BASEL II Compliance

BASEL II requires a new level of risk management and accountability. As a result, the vital role security information and event management (SIEM) plays in establishing and maintaining internal controls has never been greater. Financial institutions must institute log monitoring and vulnerability assessments as a critical part of their IT internal control systems.

Both European and international financial institutions must comply with BASEL II. Covered institutions must have methods to maintain audit trails and to log the possible altering of electronic records to demonstrate risk levels to counterparties across borders. Network Intelligence has mapped best practices and reports to help banks and affected financial institutions comply with BASEL II regulatory review processes. To address requirements, Network Intelligence meets the following objectives:

- **Access Control** monitors attempts to access the company’s financial reporting system or the data that feeds the system.
- **Configuration Control** monitors the configuration, policies and software installed on systems covered by BASEL II and all systems with access to that system.
- **Malicious Software** capabilities detect, collect and report malicious activities caused by viruses or other malicious code from a wide variety of sources with centralized analysis
- **Policy Enforcement** verifies that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- **User Monitoring and Management** creates a complete audit of the activities of non-employees with access to private data and takes steps to minimize the risk from compromised accounts.
- **Environmental and Transmission Security** involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measures such as VA scans. Additional monitoring is required to ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

To achieve and maintain compliance in those areas, companies must use the following product capabilities with respect to the data collected by the Network Intelligence Log Management solution:

- **Collect, Protect and Store** data in a non-filtered, non-normalized fashion that is preserved in an efficient and protected manner.
- Establish **Baseline** levels of activity for the entire system and network environment to define “normal activity” and detect unusual levels of activity.
- Efficiently generate the summary and detailed **Reports** spanning the data retention periods mandated by BASEL II.
- **Alert** companies to deviations from baseline activities and complex patterns of malicious activity across multiple, disparate devices.
- **Forensic Analysis** of systems correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment.
- Establish **Incident Management** capabilities for close monitoring and correction of violations to make sure they are recorded, escalated and corrected in a timely and thorough manner.

These functions ensure that the administrative, physical and technical controls demanded by the BASEL II regulation are maintained. Network Intelligence solutions address all of the technical standards required.

## The Network Intelligence Internet Protocol Database

Using its advanced LogSmart® Internet Protocol Database™ (IPDB) architecture that is deployed in hundreds of enterprises worldwide, Network Intelligence is able to capture All the Data™ from network, security, host, application and storage layers across the enterprise. The LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization — from the IT department, to the security department, to the compliance and risk officers, and executive management.

The benefits of the LogSmart IPDB include:

- Designed to store and work efficiently with unstructured data natively, without any filtering or data normalization.
- Maintains a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered — unlike most data schemas used in RDBMS-based solutions.
- No agents are required.
- Distributed peer-to-peer architecture enables high scalability and performance.

## Compliance Alerts

Network Intelligence provides the ability to automatically generate alerts based on non-compliance with an observed baseline. This means, should a particular control deviate above certain thresholds, an alert can be triggered and action can be taken to maintain compliance.

REPORT TITLE	DESCRIPTION
BASEL II – Computer Account Logon Activity - Windows Detail	This report lists all logon activity for all monitored Windows domains and systems. This report is specific to monitored Windows systems, but provides a greater level of detail than the Computer Account Logon Activity report.
BASEL II – Computer Account Logon Activity	This report lists all local and remote logon activity for all monitored Windows, HP-UX, AIX Unix, Sun Solaris and Red Hat Linux systems.
BASEL II – Computer Account Status by Account	This report lists all logon activity for specific user accounts. The user accounts in question should be listed as run time parameters, and multiple values can be specified by listing each value in single quotes and separating them by commas.
BASEL II – Control of Collected Evidence - Windows Detail	This report lists all changes and object level access Events to all collected evidence. This report requires that all evidence be contained within directories included in a device group called "Rules for Evidence", and that object level auditing be enabled on these directories. This report is specific to monitored Windows systems, but provides a greater level of detail than the standard Control of Collected Evidence report.
BASEL II – Control of Collected Evidence	This report lists all changes and object level access Events to all collected evidence. This report requires that all evidence be contained within directories included in a device group called "Rules for Evidence", and that object level auditing be enabled on these directories.
BASEL II – Control of Human Resources Data - Windows Detail	This report lists all changes and object level access Events to the device group "HR". This report requires that all software and Human Relations data be contained within a device group, and object level auditing be enabled on the directories containing the Human Relations data. This report is specific to monitored Windows systems, but provides a greater level of detail than the standard Control of Human Resources Data report.
BASEL II – Control of Human Resources Data	This report lists all changes and object level access Events to the device group "HR". This report requires that all software and Human Relations data be contained within a device group, and object level auditing be enabled on the directories containing the Human Relations data.
BASEL II – Control of Operational Software - Windows Detail	This report lists all changes and object level access events to the device group "Operational Software". This report requires that all Operational Software be contained within a device group, and object level auditing be enabled on the directories containing the Operational Software and data. This report is specific to Windows devices but provides more detail than the standard Control of Operational Software report.
BASEL II – Control of Operational Software	This report lists all changes and object level access Events to the device group "Operational Software". This report requires that all Operational Software be contained within a device group, and object level auditing be enabled on the directories containing the Operational Software and data.
BASEL II – Control of System Audit Data - Windows Detail	This report lists all changes and object level access events to the software and data used to perform system audits. This report requires that the software, source data and result data be contained within a device group, and object level auditing be enabled on the containing directories. This report is specific to Windows devices but provides more detail than the standard Control of System Audit Data report.
BASEL II – Control of System Test Data - Windows Detail	This report lists all changes and object level access Events to the systems and data used in the testing of Operational Software security. This report requires that all system test data be contained within a device group, and object level auditing be enabled on the directories containing the system test software, source data and test results.
BASEL II – Control of System Test Data	This report lists all changes and object level access Events to the systems and data used in the testing of Operational Software security. This report requires that all system test data be contained within a device group, and object level auditing be enabled on the directories containing the system test software, source data and test results.
BASEL II – External Contractors Report - Windows Detail	This report lists all changes and object level access Events to the device group "External Contractor Access". This report requires that all computers, software, source data and result findings be contained within a device group, and object level auditing be enabled on the directories containing this data.
BASEL II – External Contractors Report	This report lists all changes and object level access Events to the device group "External Contractor Access". This report requires that all computers, software, source data and result findings be contained within a device group, and object level auditing be enabled on the directories containing this data.
BASEL II – Financial Data Access - Windows Detail	This report lists all successful and failed access attempts for all financial data. This report requires that all financial data be contained within a device group, and object level auditing be enabled on the directories containing the financial data.
BASEL II – Financial Data Access	This report lists all successful and failed access attempts for all financial data. This report requires that all financial data be contained within a device group, and object level auditing be enabled on the directories containing the financial data.
BASEL II – Operation Change Control Report - Windows Detail	This report lists all configuration and policy changes for the Financial Operational infrastructure. This report is restricted to only Windows devices, but delivers a greater level of detail than the standard "Operation Change Control Report".
BASEL II – Operation Change Control Report	This report lists all configuration and policy changes for the Financial Operational infrastructure.
BASEL II – Password Changes and Expirations	This report lists all manual and automatic password change and expiration events. This includes Windows, Sun Solaris, Red Hat Linux, HP-UX and AIX operating systems.
BASEL II – Source Code Access - Windows Detail	This report lists all changes and object level access Events to the device group "Source Code". This report requires that the source code for all custom software and commercial software customization be contained within a device group, and object level auditing be enabled on the directories containing the source code
BASEL II – Source Code Access	This report lists all changes and object level access Events to the device group "Source Code". This report requires that the source code for all custom software and commercial software customization be contained within a device group, and object level auditing be enabled on the directories containing the source code.
BASEL II – User Activity from External Domains	This report details all activities of non-domain authenticated users. All authenticated domains are identified in run time parameters, and multiple domains can be contained within single quotes and separated by commas.
BASEL II – Control of System Audit Data	This report lists all changes and object level access Events to the software and data used to perform system audits. This report requires that the software, source data and result data be contained within a device group, and object level auditing be enabled on the containing directories.
BASEL II – Malicious Software Activity	This report lists all malicious software activity for all monitored devices.
BASEL II – User Activity from External Domains - Windows	This report lists all logon activity for specific user accounts. The user accounts in question should be listed as run time parameters, and multiple values can be specified by listing each value in single quotes and separating them by commas.
BASEL II – Computer Account Status by Account - Windows	This report details all activities of non-domain authenticated users. All authenticated domains are identified in run time parameters, and multiple domains can be contained within single quotes and separated by commas.