

## ***Basel II Compliance***

Basel II establishes minimum capital requirements for banking organizations to reduce operational risks, defined as the risk of loss resulting from inadequate or failed internal process, people and systems or from external events. To achieve compliance with Basel II requirements, organizations must identify, assess, monitor and control their operational risk, much of which occurs at the endpoint.

## ***Sanctuary Helps Public Companies Comply with Basel II for Endpoint Security***

Sanctuary helps organizations identify, assess, monitor and control operational risk at the endpoint by providing a detailed audit trail of all device and application execution attempts, by tracking data that is copied to and from removable devices and by controlling what data is allowed to be copied to a device at the file level.

By employing a whitelist approach, Sanctuary is uniquely capable of enforcing application and device usage and control policies, which enables only authorized applications and devices to run or connect to a network, server, terminal services server, laptop, thin client or desktop – facilitating security and systems management, while providing necessary flexibility to the organization to easily enable the use of new/upgraded applications or devices.

Through policy-based control at the endpoints to monitor and control the inbound and outbound flow of sensitive information, Sanctuary complements organizations' Basel II compliance strategy by implementing the proper internal safeguards around application and device use:

### **Basel II Requirement - *Monitoring and Reporting***

“The bank should establish an adequate system for monitoring and reporting risk exposures.”

### ***How Sanctuary Addresses Basel II Requirements***

Sanctuary provides a detailed audit trail of all device and application execution attempts and tracks all data that is copied to and from removable devices.

### **Basel II Requirement - *Internal Control Review***

“The bank’s internal control structure is essential to the capital assessment process. The bank’s board of directors has a responsibility to ensure that management establishes a system for assessing the various risks, develops a system to relate risk to the bank’s capital level, and establishes a method for monitoring compliance with internal policies.”

### ***How Sanctuary Addresses Basel II Requirements***

Sanctuary enables the enforcement of device and application use and control policies that are established by an organization. Risk can be assessed through the monitoring of all device and application execution attempts as well as monitor the amount of data and file types that are copied

to and from removable devices.

#### **Basel II Requirement - [Annex 7 \(1/3\) - Internal Fraud](#)**

Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party

- Unauthorized Activity
- Theft and Fraud

#### **[How Sanctuary Addresses Basel II Requirements](#)**

Sanctuary enforces policies that control device and application use to prevent internal theft and fraud. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC. This capability significantly reduces the risk of insiders stealing sensitive or confidential data.

#### **Basel II Requirement - [Annex 7 \(1/3\) - External Fraud](#)**

Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law by a third party

- Theft and Fraud
- Systems Security

#### **[How Sanctuary Addresses Basel II Requirements](#)**

Sanctuary enforces policies that control device and application use to prevent external theft and fraud. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC. This capability prevents malware and spyware from proliferating at the endpoint, which if left unmanaged could expose data to theft or disrupt an organization's network.

#### **Basel II Requirement - [Annex 7 \(1/3\) - Annex 7 \(2/3\) – Clients, Products and Business Practices](#)**

Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product

- Suitability, Disclosure and Fiduciary
- Improper Business or Market Practices
- Product Flaws

### ***How Sanctuary Addresses Basel II Requirements***

Sanctuary enforces policies that control device and application use to protect the confidentiality and integrity of clients data from unintentional or negligent users. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC. This capability prevents malware and spyware from proliferating at the endpoint, and protects against users from improperly copying specific information onto unauthorized devices which if left unmanaged could expose data to theft or disrupt an organization's network.

#### **Basel II Requirement - *Annex 7 (3/3) – Business Disruption and System Failures***

Losses arising from disruption of business or system failures

- Systems

### ***How Sanctuary Addresses Basel II Requirements***

Sanctuary enforces policies that control device and application use to prevent network system disruption or failure. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC. This capability prevents malware and spyware from proliferating at the endpoint, which if left unmanaged could disrupt an organization's network.

#### **Basel II Requirement- *Annex 7 (3/3) – Execution, Delivery and Process Management***

Losses from failed transaction processing or process management, from relations with trade counterparties and vendors:

- Transaction Capture, Execution and Maintenance
- Monitoring and Reporting
- Customer Intake and Documentation
- Customer/Client Account Management

### ***How Sanctuary Addresses Basel II Requirements***

Sanctuary enforces policies that control device and application use to enable the transmission, integrity, confidentiality and retention of data without disruption, corruption or loss.

