

# Splunk App for IBTRM v3

Addressing the Internet Banking and Technology Risk Management (IBTRM) Guidelines from the Monetary Authority of Singapore

## The Challenges of Risk Management

In 2008, the Monetary Authority of Singapore (MAS) updated the Internet Banking and Technology Risk Management (IBTRM) Guidelines. The Guidelines aims to assist banks in:

- Establishing a sound and robust technology risk management framework
- Strengthening system security, reliability and availability
- Deploying strong cryptography and authentication mechanisms to protect customer data and transactions

Quoting the IBTRM v3, “Banks face the challenge of adapting, innovating and responding to the opportunities posed by computer systems, telecommunications, networks, and other technology-related solutions to drive their businesses.” The on-going understanding of risk to the bank translates to higher levels of trust from customers across the globe and differentiation from other banking centers.

The new version of IBTRM provides expanded guidance for combating cyber threats and attacks, including emerging cyber exploits such as middleman attacks. It also recommends enhanced technology risk management requirements for strengthening system, network and infrastructure security, and articulates stronger procedures for system development and security testing.

## Why Splunk?

### Operational Intelligence and Continuous Monitoring

Splunk Enterprise can collect any time-stamped ASCII text data in real-time without the use of special connectors typically associated with log collection and security and event management systems. Splunk allows the user to add knowledge from external sources and view this information in reports and dashboards.

### Using Splunk for IBTRM compliance

The IBTRM requires that specific banking industry vertical strategies are established to meet the Security and Control objectives of:

- Data Confidentiality
- System Integrity
- System Availability
- Customer and Transaction Authenticity
- Customer Protection

By using Splunk as a central repository for security and application log data, as well as other third-party data, specific IBTRM requirements can be met. For example, log data may indicate a breach of data confidentiality on several systems but the log data doesn't prioritize high value assets from those that are not. The question becomes where to start. By integrating

data from an asset management system that contains the system priority classifications, the user is able to work to remediate issues based on set priorities.

## Non-administrative IBTRM Security and Control Objectives (4.0):

### Data Confidentiality (4.1)

Splunk provides the ability to monitor log data for confidential information such as credit cards. In some cases this information is needed when troubleshooting application issues. To use this data while protecting confidential information, Splunk can mask portions of the sensitive information from non-authorized users.

Splunk can be used to monitor system configuration to make sure that particular encryption settings are in place for SSL and SSH. Configuration changes can also be monitored to ensure none take place outside of established time windows. Splunk can also log user access records and generate reports to provide an audit trail for cryptographic key access.

### System Integrity (4.2)

Banking application logs can be monitored in real time to ensure that transactions happen in sequence and that the average time for banking transactions is used as a key performance metric. Also, application error rates can be monitored over time to indicate potential problems. This is particularly important when new versions of custom applications are tested and released to production. Log data records and transaction access logs comprise a comprehensive solution for PCI secure log collection, and as part of this the logs are signed to prevent tampering.

### System Availability (4.3)

Log data contains important information that can indicate the reliability and usage of systems in the enterprise architecture. Monitoring systems for CPU utilization over time helps with capacity planning, improves reliability and can offer an understanding of the resiliency of the architecture. Metrics dashboards to track traffic volumes and transactions on a continual basis allow you to not only monitor the network and applications but also provide higher levels of customer satisfaction.

### Customer and Transaction Authenticity (4.4)

Monitoring customer transactions in real-time for correct and complete authentication is the key tenant of IBTRM customer transaction authenticity control requirement. Splunk was built with this in mind and can monitor transactions represented in log data that mean transactions above pre-set values, creation of new account linkages, registration of third-party payee details, changes in account details and changes to fund transfer limits. Through the Splunk look-up feature, account limitation details that may reside in other parts of the infrastructure can be viewed in reports and dashboards along with customer transaction details.

It's also important to monitor the transactions for total time as a key infrastructure metric. This can effect customer service and indicate security or application issues related to risk.

#### Customer Protection (4.5)

The popularity of on-line banking continues to grow at a rapid pace in maturing markets all over the world. Customer protection through proper authorization is a requirement prior to accessing sensitive data. Banks have become a popular target for phishing, spoofing, spamming, viruses, worms, Trojan horses, trapdoors, key loggers, spyware, and other types of attacks. These sorts of attacks can create financial and reputation losses.

The Zeus malware is an example that has been seen in a variety of variants each potentially more potent than the last. Zeus started out as malware that specifically targeted customer-banking passwords stored on their PCs but has more recently been seen on eastern-bloc ATM machine operating systems collecting account information and PIN numbers. Splunk can be configured to monitor malware patterns and reduce risk.

In many instances root cause analysis requires the security team to view log data that may contain private data. Splunk has the ability obfuscate credit card and PIN numbers so that the user can view the data for forensics purposes without violating payment card industry (PCI) requirements.

### Other Benefits of Using Splunk for IBTRM

Security system and application monitoring go hand-in-hand when implementing risk reduction. Anything impacting the acquisition of customers, revenue, expenses or reputation should be examined and where possible mitigated.

The Splunk ability to collect any IT data means that application and security system data can be viewed together for complete investigations of customer risk related events. Splunk can be implemented in ways that compliment the core security components of IBTRM:

- Monitor physical security access logs for unauthorized access to areas where critical data is stored (5.1 HR Management)
- Implement Splunk native capabilities to ensure role-based access for segregation of duties (5.1 HR Management)
- Collect, monitor and alert on access control issues related to employees, service providers, and others (5.1 HR Management)
- Utilize audit capabilities to monitor users of Splunk to ensure timely use and viewing of report data (5.1 HR Management)

- Monitor security system data suspicious traffic, intrusion attempts, and violations of bank security policies (Security Practices 5.2)
- Monitor file system time/date changes for activities that happen outside of authorized change windows (Security Practices 5.2)
- When developing applications, Splunk can be used to troubleshoot bugs and system errors to detect application vulnerabilities (System Development Life Cycle 6.1)

### Features

- Indexes machine data across the IT infrastructure
- Monitors configuration file changes
- Automates compliance reporting across all components
- Flexible and fast to meet auditor data request in seconds
- Accelerates mandated daily audit trail review with event classification, visualization and tagging
- Flexible alerting and reporting across machine data
- Secure, policy-based remote access to IT data mitigates the impact and violations of access restrictions
- Lets you share alerts/data with service providers & other tools
- Alerts can trigger automated actions to immediately react to certain conditions.
- Accelerated reporting across compliance mandated controls, from firewall configuration to password

### Free Download

Download [Splunk](#) for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting [sales@splunk.com](mailto:sales@splunk.com).