Trust Management in Monitoring Financial Critical Information Infrastructures and The Policy Compliance with Nagios XI

Jorge Higueros
Jorge.higueros@consulmatic.com
The Financial System

Include:

- The banking system,
- Financial institutions,
- The payment system,
- Exchanges,
- The money supply,
- Financial regulations,
- As well as accounting standards and regulations in around the world
Let's see

Nagios Interacts with:

- BIA
- Risk Analysis
- Identify Strategic
- BCP
- Update Planning
- Security Plans
- Capacity Planning
Components IT Infrastructure

- Compatibility
- Connectivity
- Modularity
- IT personnel
- Strategic IT-business
- Alignment
Properties

- Flexibility of IT infrastructure describes the degree to which its resources are sharable and reusable and how rapidly and effectively the IT organization is able to respond to emergent needs or opportunities.
IT Capability

- Capability is a combination of functionality and connectivity
- Between Levels and Gaps

<table>
<thead>
<tr>
<th>IT CAPABILITY LEVELS AND GAPS</th>
<th>Basic</th>
<th>Standardized</th>
<th>Rationalized</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IDENTITY &amp; ACCESS MANAGEMENT</strong></td>
<td>No common identity management model</td>
<td>Identity management for user identification</td>
<td>Centralized configuration &amp; authentication</td>
<td>Centralized with automated procurement</td>
</tr>
<tr>
<td><strong>DESKTOP ENGINEERING</strong></td>
<td>No desktop standards, many images</td>
<td>Automated patch management</td>
<td>Manual reference image</td>
<td>Automated reference image</td>
</tr>
<tr>
<td><strong>SECURITY, NETWORKING &amp; MONITORING</strong></td>
<td>No standards</td>
<td>Antivirus central firewall</td>
<td>Secure remote access server monitoring</td>
<td>Centralized with automated procurement</td>
</tr>
<tr>
<td><strong>DISASTER RECOVERY</strong></td>
<td>No formal procedures in place</td>
<td>Mission critical server backup &amp; recovery</td>
<td>All servers</td>
<td>Centralized with automated procurement</td>
</tr>
<tr>
<td><strong>SECURED MESSAGING INFRASTRUCTURE</strong></td>
<td>Multiple messaging standards</td>
<td>Unified directory for messaging, spam control, server health monitoring</td>
<td>Secure email access across channels</td>
<td>Secure email access across devices</td>
</tr>
</tbody>
</table>
The Diversity & Flexibility Alliance can help your firm or legal department develop strategies and resources to support diversity and flexibility.
How is the financial IT infrastructure

▶ Changing
▶ Large maintenance

▶ Growing

Diagram showing infrastructure views with layers:
- Business Process
- Information
- Application(s)
- Server(s)
- Building/Facility
- Utility Provider

Infrastructure for business analyst
Infrastructure for end user
Infrastructure for system manager
How is the environment

- Businesses Process
- Quality of service
- Downtimes
Infrastructure Management in the Past

- Manual Optimizing resources
- Issues management process
Infrastructure Management with Nagios XI
Goals are...

- High availability = All Services 99.99% uptime
- Prevention
With more financial applications subject to 24/7 business service level agreements, banks are working to ensure continuity of IT operations as well as reduce the cost of the bank’s operational resiliency strategy.
Nagios XI delivers a solution to ensure high availability and centralized management across the Financial Institutions in numerous applications and heterogeneous platform technologies for branch applications, call centers, payments and trading operations, as with other core banking system.
Nagios Objectives

- Eliminate impact of planned downtime such as upgrades and maintenance operations
- Reduce impact of unplanned downtime with local or remote site failover capabilities
- Provide improved end-to-end availability across application dependencies and databases
- Reduce operations costs through a standardized platform for Unix, Linux, Windows systems
Nagios in the Financial World
A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries. There are many possible scenarios which should be considered.
Business Impact Analysis (BIA)

The BIA should identify the operational and financial impacts resulting from the disruption of business functions and processes. Impacts to consider include:

- Lost sales and income
- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans
A risk assessment is a process to identify potential hazards and analyze what could happen if a hazard occurs. A business impact analysis (BIA) is the process for determining the potential impacts resulting from the interruption of time sensitive or critical business processes.
Identify Strategic With Nagios

Delivery Plans

-QA/Validation
-User Training
-Knowledge Transfer

-Program Vision
-Project Planning
-Success Metrics

-System configuration
-Integration with 3rd party systems
-Optimization & Best Practices

PLAN

DEPLOY

PROGRAM DELIVERY SYSTEM

DESIGN

BUILD

Nagios
World Conference
North America

#NagiosCon13
With Nagios can identify the most critical components in the infrastructure like:

- Critical personnel, facilities, computer systems, operations, and equipment;
- Priorities for processing, recovery, and mitigation;
- Maximum downtime before recovery of operations; and
- Minimum resources required for recovery.

Long-term goals and objectives may include:

- Management's enterprise-wide strategic plan;
- Coordination of personnel and activities;
- Budgetary considerations; and
- Supervision of third-party resources.
Government Regulations

Latin American Cases
Chapter 1, Article 2. Definitions.

Technological risk management is the process of identifying, measuring, monitoring, control, prevent and mitigate technological risk.

Technological risk: proactive prevention to operational failures

Chapter 2 - Section 6. Risk Management Unit

c) Monitor the technological risk exposure and maintain historical records of such monitoring and measuring technology risk

Chapter 3 - Article 10. Outline of business information

Article 11. Inventories of IT infrastructure, information systems and databases

Article 13. Monitoring infrastructure, information systems and databases

Article 14. Acquisition, maintenance and implementation of IT infrastructure, information systems and databases

Article 15. IT Service Management

Chapter 4 - Article 17. Security management information

c) Monitoring of security information;
Risk information technology is the potential for economic losses derived from an event related to the technological infrastructure, access or use of the technology, which affects the development of business processes or risk management of the bank, to violating the confidentiality, integrity, availability, efficiency, reliability, compliance or timely use of information.
CHAPTER V. - OPERATIONAL RISK MANAGEMENT

(included with Resolution No JB-2005-834 of October 20, 2005)
Nagios and Policy Compliance
Some Examples

- Sarbanes-Oxley
- COBIT 5
- COSO II
- ITIL V3
- ISO 20000
- Government Compliance
Passed in 2002, the Sarbanes-Oxley (SOX) or Public Company Accounting Reform and Investors Protection Act is focused on protecting shareholders. Nagios can help your organization in areas ranging from monitoring systems and services to assisting in verifying they are in a trusted state.
Sarbanes-Oxley

**ROI**
Documented client results include:
- **60%** Reduction in total SOx project time
- **45%** Year-over-year reduction of ineffective controls
- **55%** Increase in operational audit activity
- **95%** Less time on SOx analysis and reporting
- **50%** Decrease in external auditor review time
COBIT 5

- COBIT’s main goal is to align the business drivers of an organization with the management of their information technology.

- Business objectives are achieved.

- Undesired events are prevented or detected and corrected.
COBIT 5

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement

- BA001 Manage Programmes and Projects
- BA002 Manage Requirements Definition
- BA003 Manage Solutions Identification and Build
- BA004 Manage Availability and Capacity
- BA005 Manage Organisational Change Enablement
- BA006 Manage Changes
- BA007 Manage Change Acceptance and Transitioning
- BA008 Manage Knowledge
- BA009 Manage Assets
- BA010 Manage Configuration

Deliver, Service and Support

- DS001 Manage Operations
- DS002 Manage Service Requests and Incidents
- DS003 Manage Problems
- DS004 Manage Continuity
- DS005 Manage Security Services
- DS006 Manage Business Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Source: COBIT 5, figure 16
Under the Committee of Sponsoring Organizations of the Treadway Commission (COSO), five components of the internal control framework for Nagios could be... Monitoring. While the majority of the COSO framework applies to financial processes, the Monitoring component can apply to IT and financial monitoring.
Under the PCI DSS are six groups of security principals that break down further into 12 requirements. The group most applicable to utilizing Nagios on your network is Regularly Monitor and Test Networks. Under this principal, the two requirements are:

Requirement 10 Track and monitor all access to network resources and cardholder data.

Requirement 11 Regularly test security systems and processes.
Provide policy and procedures for the security and protection of systems that create, process, store, and transmit intelligence information.

Provide administrative and system security requirements, including those for interconnected systems.

Define and mandate the use of a risk management process.

Define and mandate the use of a certification and accreditation process.

Promote the use of efficient procedures and cost-effective, computer-based security features and assurances.

Describe the roles and responsibilities of the individuals who constitute the decision-making segment of the IS security community and its system users.

Require a life-cycle management approach to implementing system security requirements.

Introduce the concepts Levels-of-Concern and Protection Level of information.
Tests are provided and periodically run to ensure the integrity of the system state. It should be noted that definition of a “system” could include the critical processes as well. In this section, we covered a few of the many compliance controls that can be bolstered utilizing Nagios. It should be clear that other compliance standards may not call out specifically for system and service monitoring (e.g., HIPPA), but Nagios can still be very valuable in these environments.