

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

Jorge Higueros

Jorge.higueros@consulmatic.com



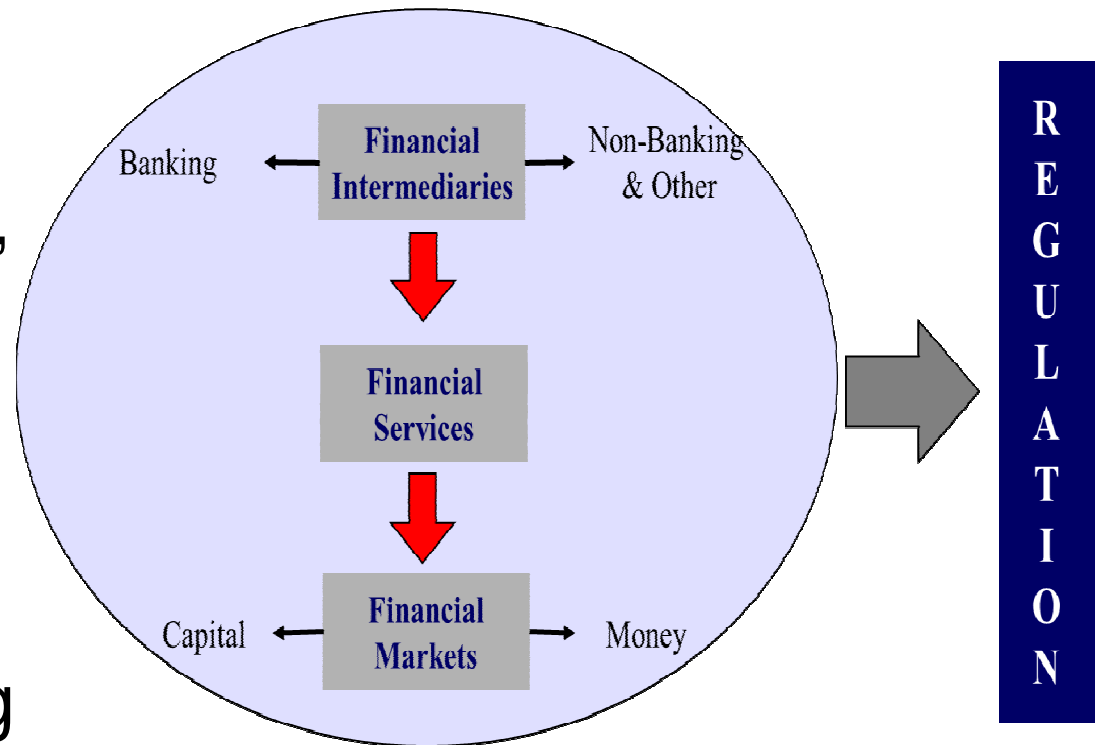
Nagios[®]

World Conference
North America

The Financial System

Include:

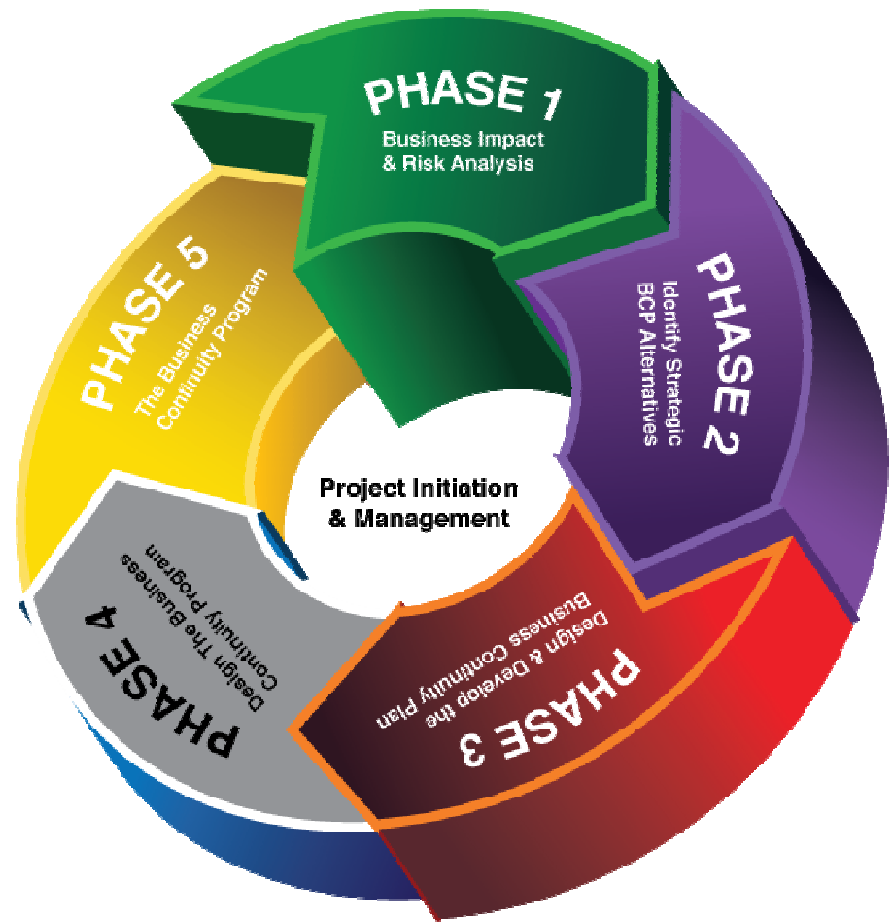
- ▶ The banking system,
- ▶ Financial institutions,
- ▶ The payment system,
- ▶ Exchanges,
- ▶ The money supply,
- ▶ Financial regulations,
- ▶ As well as accounting standards and regulations in around the world



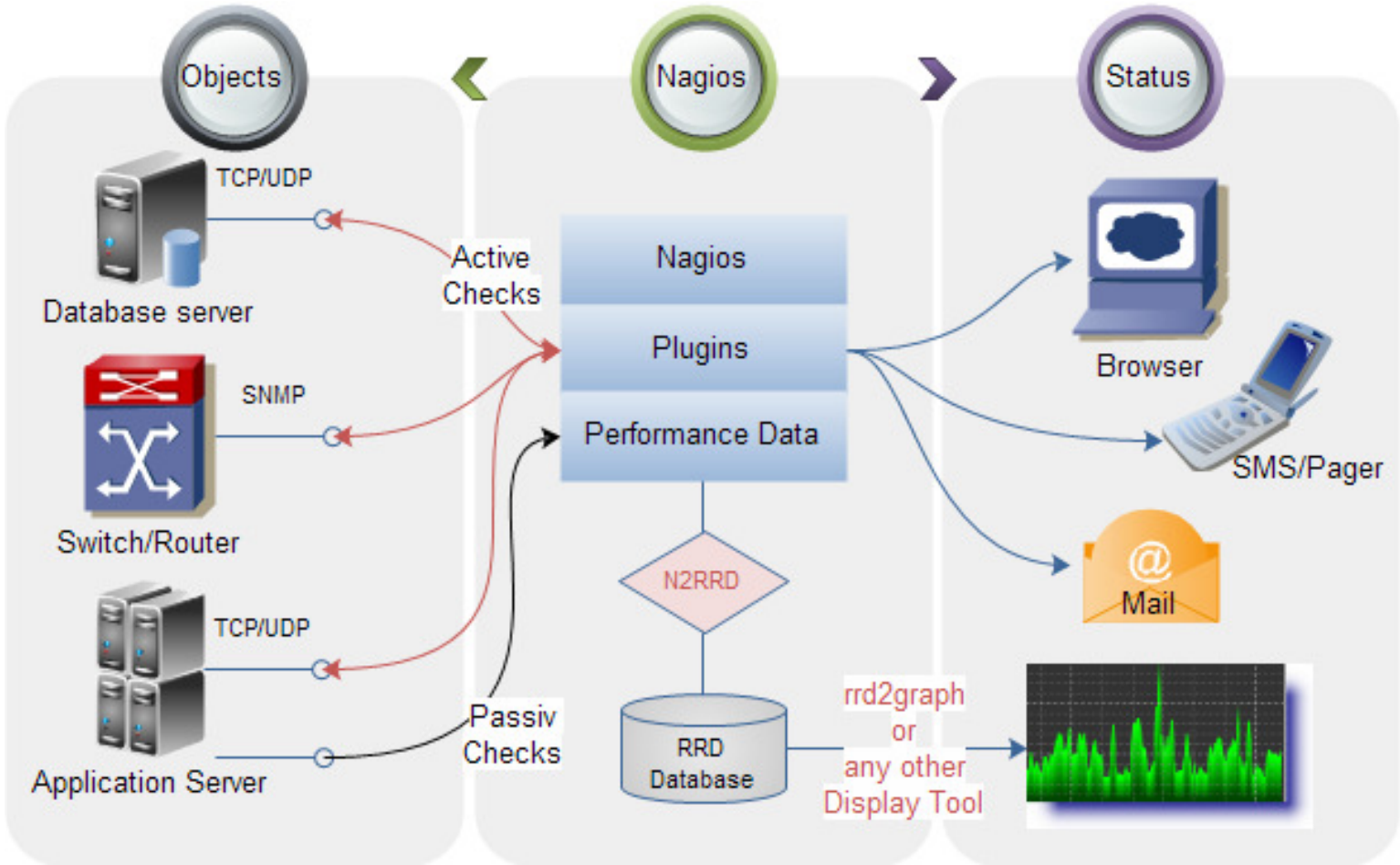
Let's see

Nagios Interacts with:

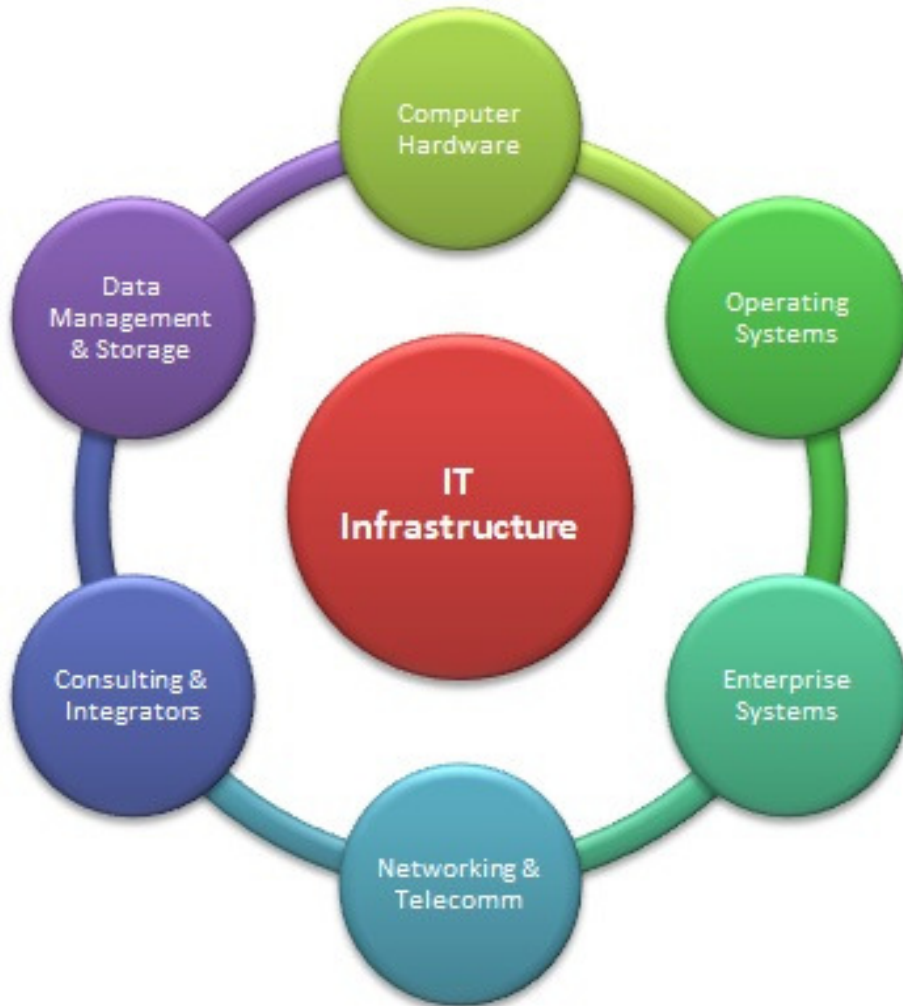
- ▶ BIA
- ▶ Risk Analysis
- ▶ Identify Strategic
- ▶ BCP
- ▶ Update Planning
- ▶ Security Plans
- ▶ Capacity Planning



Infrastructure



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

IT CAPABILITY LEVELS AND GAPS				
	Basic	Standardized	Rationalized	Dynamic
IDENTITY & ACCESS MANAGEMENT	No common identity management model	Identity management for user identification	Centralized configuration & authentication	Centralized with automated procurement
DESKTOP ENGINEERING	No desktop standards, many images	Automated patch management Standard Images	Manual reference image Automated Asset management	Automated reference image
SECURITY, NETWORKING & MONITORING	No standards	Antivirus central firewall	Secure remote access server monitoring	Centralized with automated procurement
DISASTER RECOVERY	No formal procedures in place	Mission critical server backup & recovery	All servers	Centralized with automated procurement
SECURED MESSAGING INFRASTRUCTURE	Multiple messaging standards	Unified directory for messaging, spam control, server health monitoring	Secure email access across channels	Secure email across devices Predictive monitoring

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

The Financial IT infrastructure



Strategies and Resources

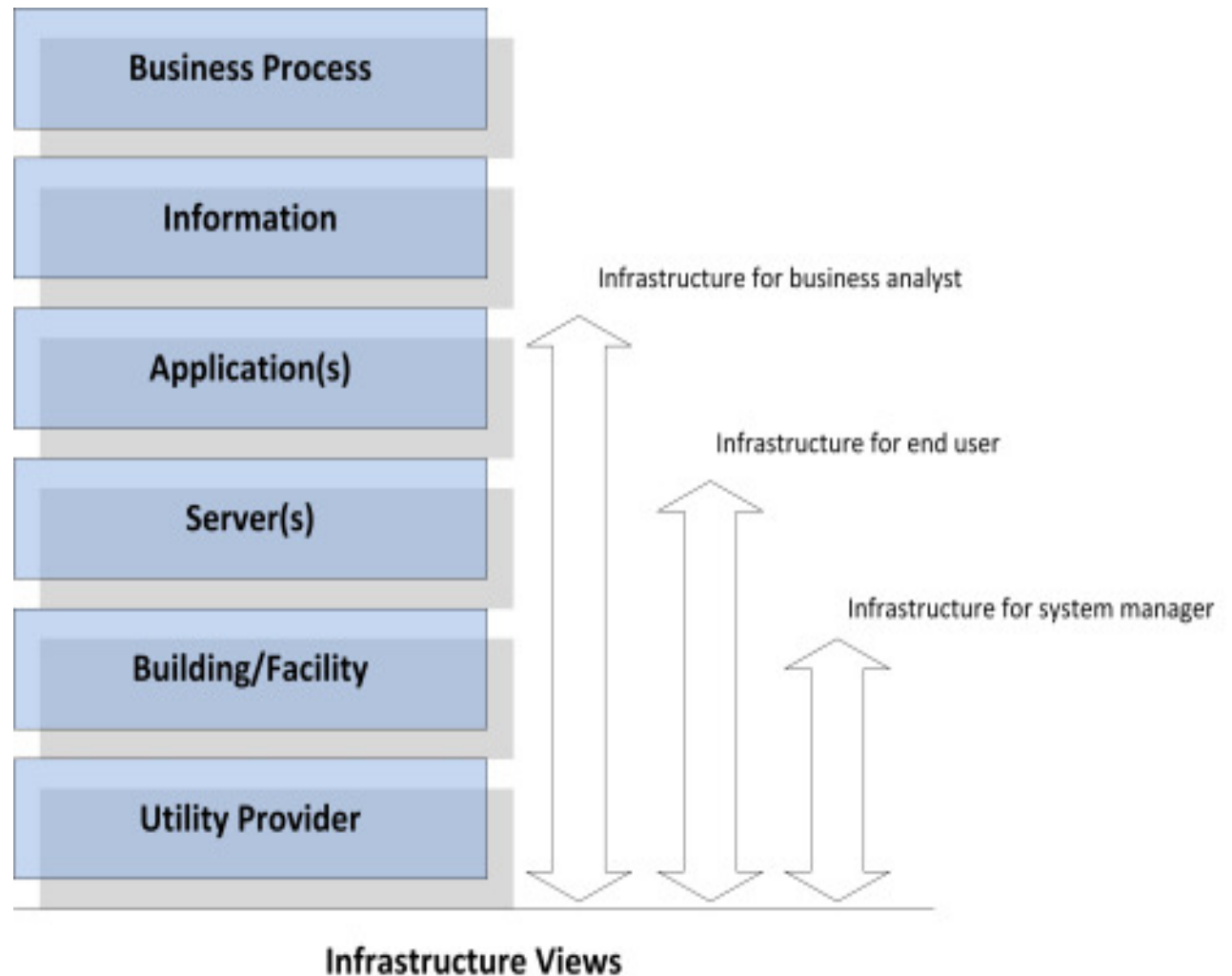
The Diversity & Flexibility Alliance can help your firm or legal department develop strategies and resources to support diversity and flexibility.

How is the financial IT infrastructure

▶ Changing

▶ Large maintenance

▶ Growing



How is the environment

▶ Businesses Process



▶ Downtimes



▶ Quality of service



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



High availability In Financial Institutions

- ▶ 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 brings the concept of High availability

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

Nagios[®]

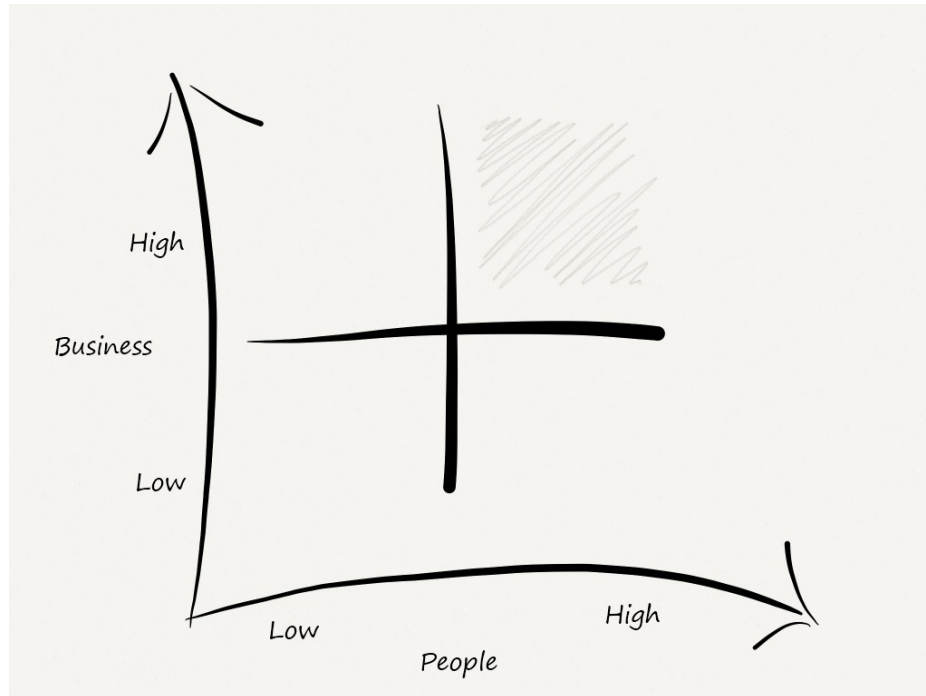


Business Impact Analysis (BIA)

- ▶ 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

		IMPACT 1: MISSING A LAW REQUIREMENT		
		HIGH (SANCTION \geq 100,000 \$)	MEDIUM (10,000 \$ \leq SANCTION < 10,000 \$)	LOW (SANCTION < 10,000 \$)
IMPACT 2: # OF CUSTOMERS	HIGH (CUSTOMERS \geq 1,000)	HIGH	HIGH	MEDIUM
	MEDIUM (100 \leq CUSTOMERS < 1,000)	HIGH	MEDIUM	LOW
	LOW (CUSTOMERS < 100)	MEDIUM	LOW	LOW

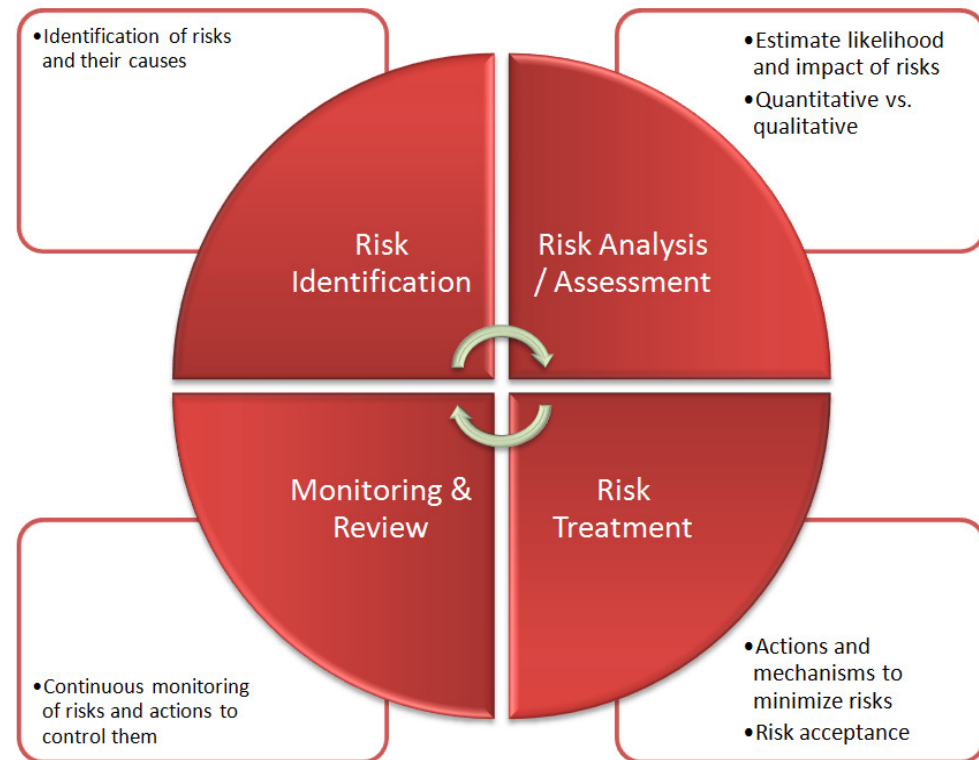
Business Impact Analysis (BIA)



- ▶ 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

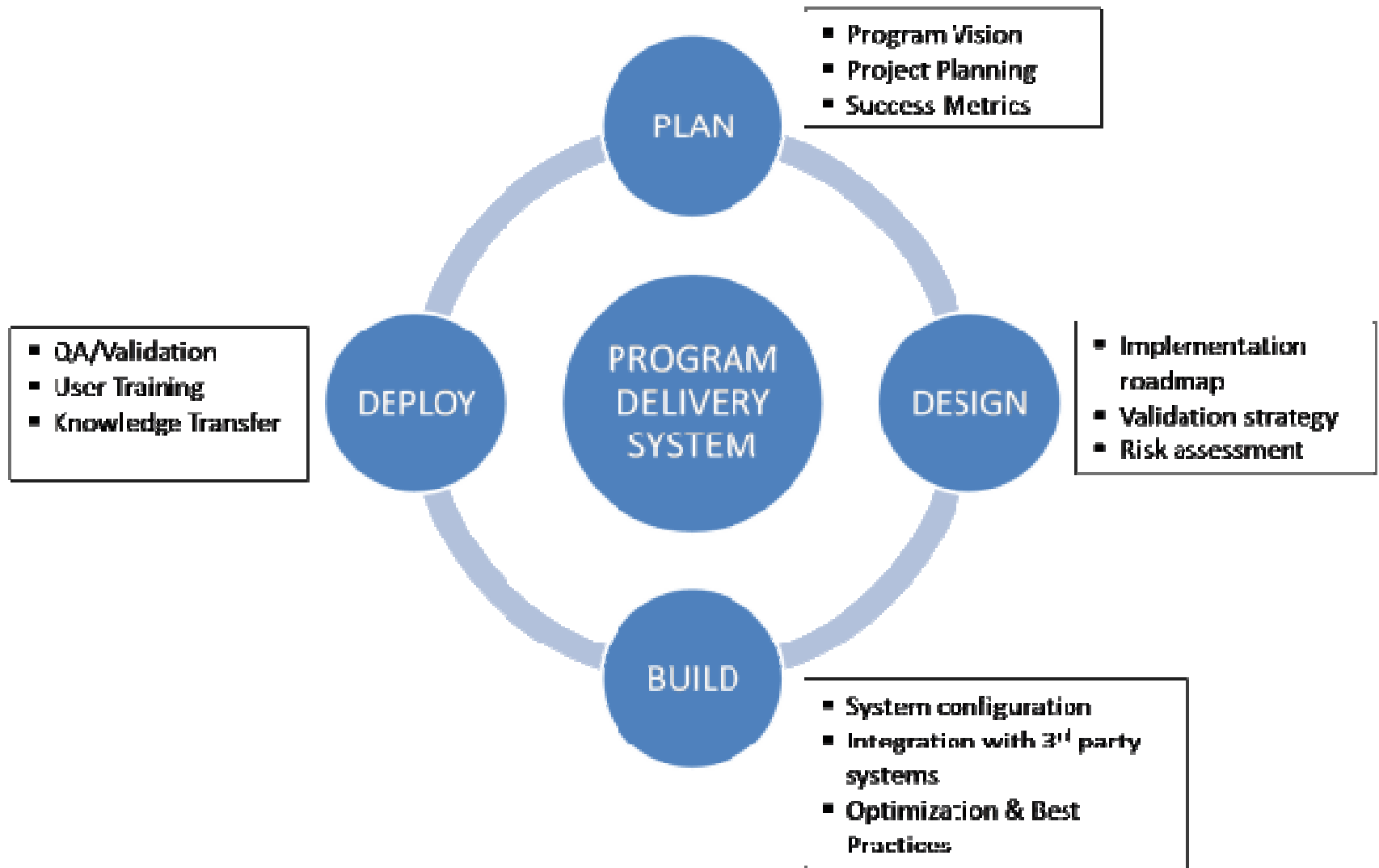
Risk Analysis

- ▶ 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



- ▶ With Nagios can identify the most critical components in the infrastructure like:
- ▶ Monitoring Data Center Recovery Alternatives



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.

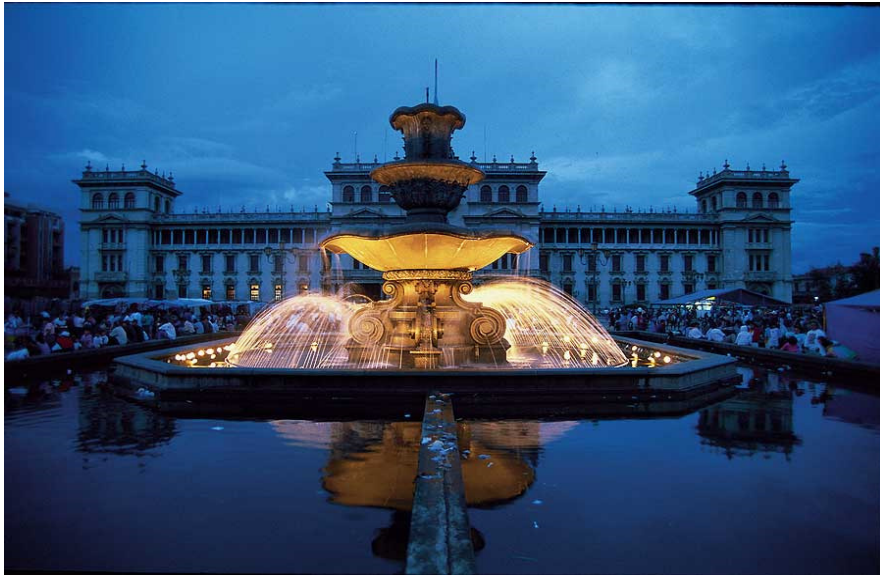
Government Regulations



Latin American Cases

Guatemala

▶ NAGIOS XI COMPLIANCE AS A TOOL FOR THE RESOLUTION JM-102-2011



▶ 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;

Panama

- ▶ Nagios Help to Acuerdo 3-2012

Risk Management Technology 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.

Ecuador

- ▶ 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



Sarbanes-Oxley

- ▶ 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



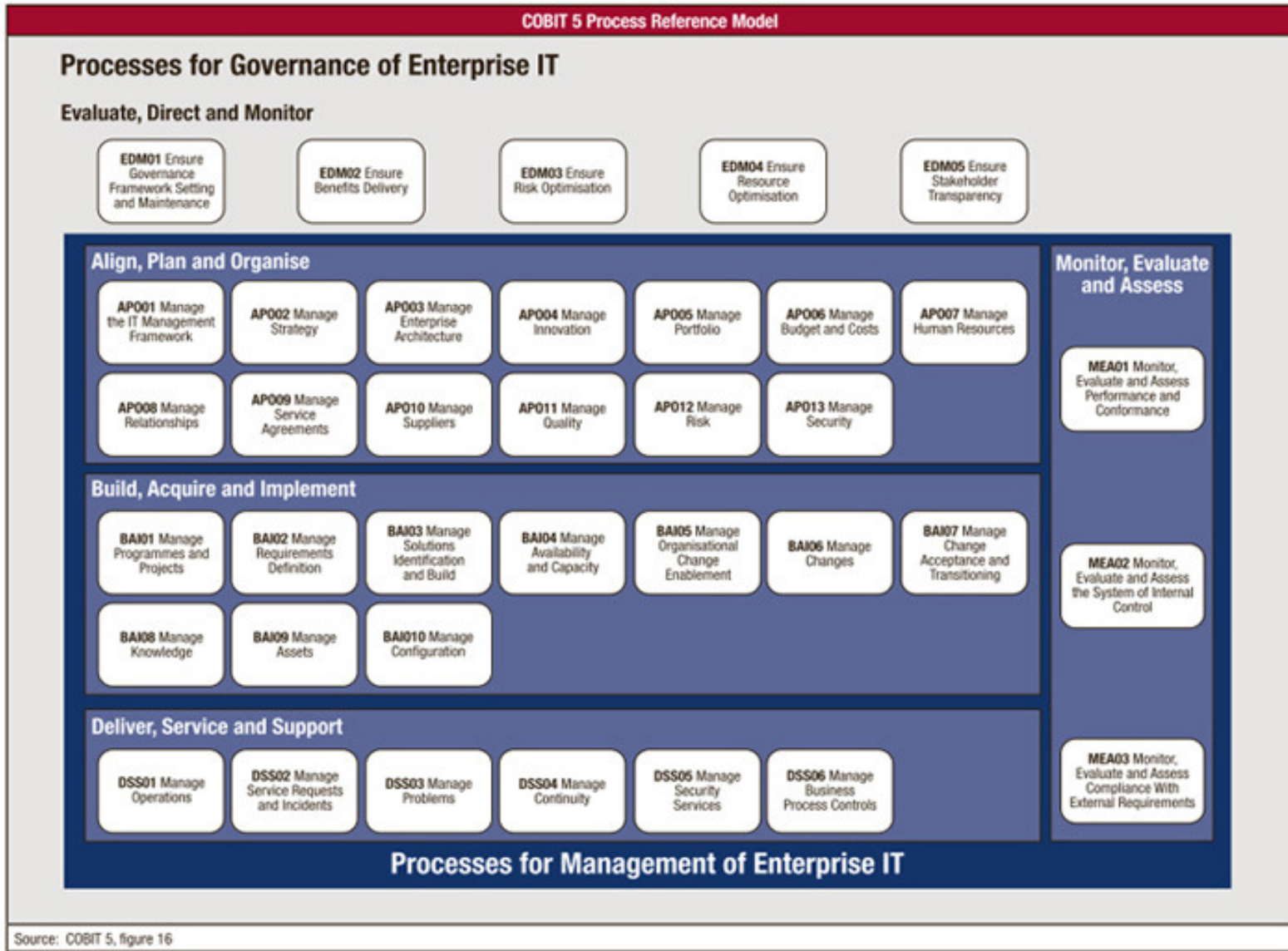
COBIT 5

▶ 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.

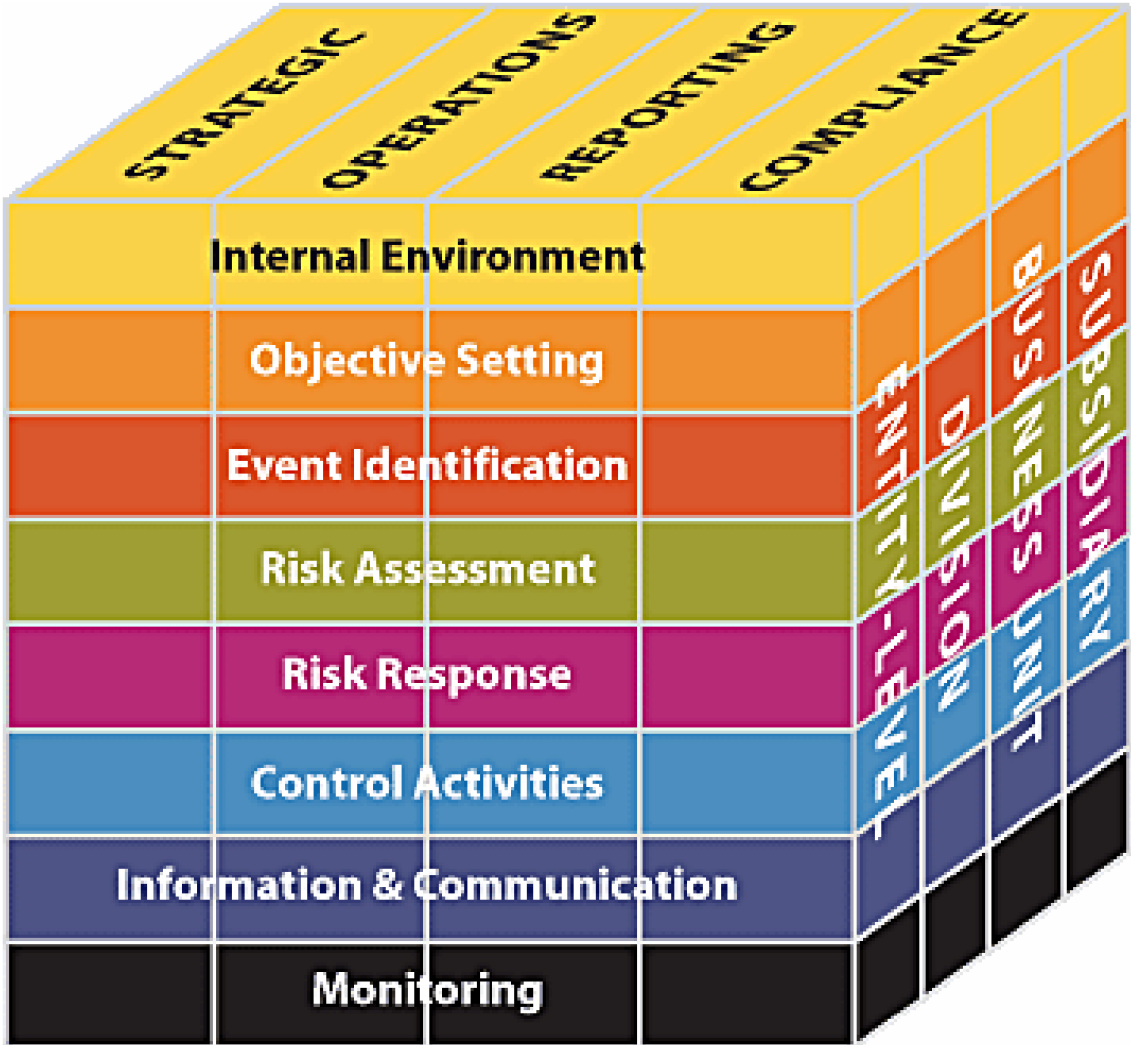
COBIT 5



COSO II

- ▶ 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.

COSO II



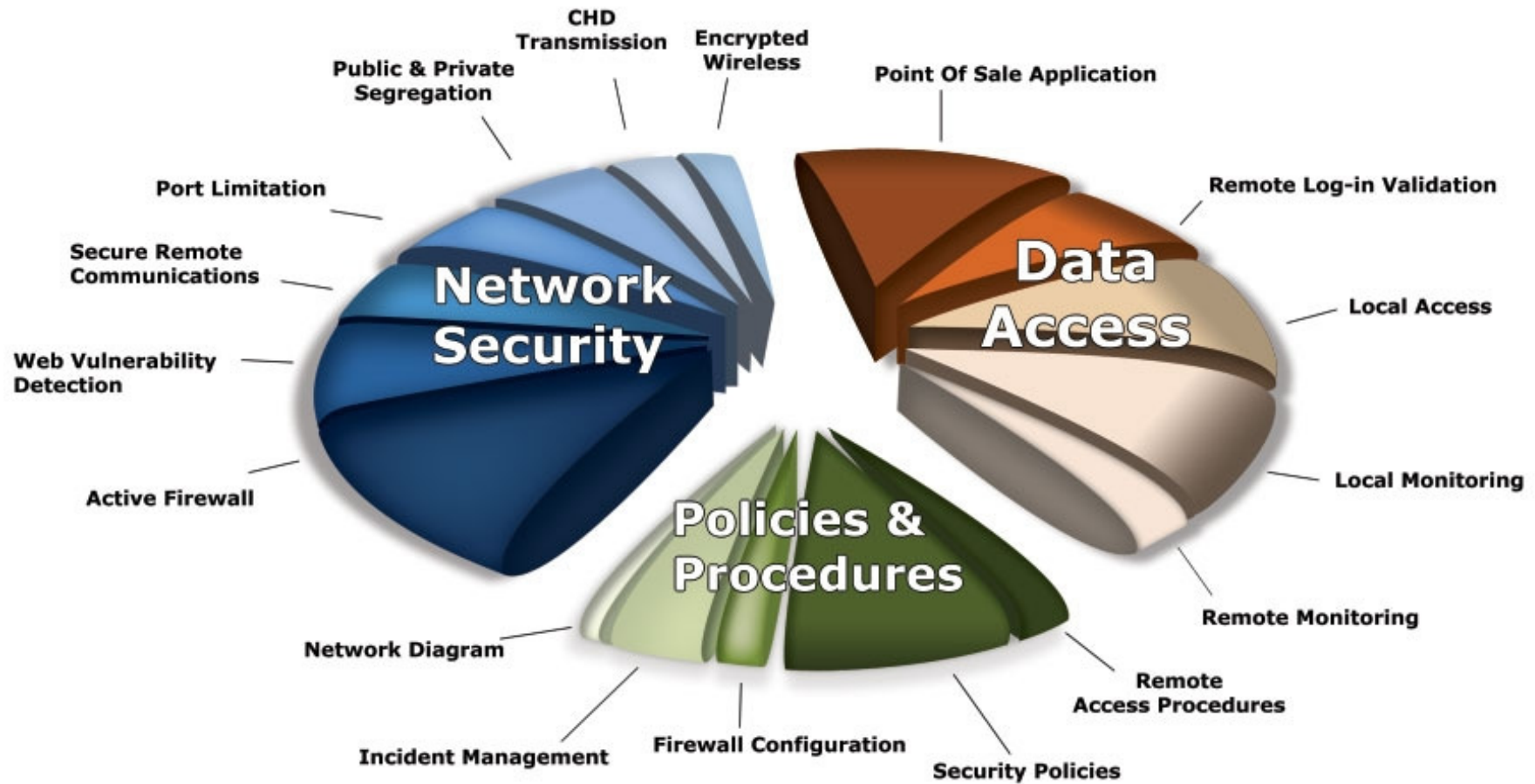
PCI DDS 2.0

▶ 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.

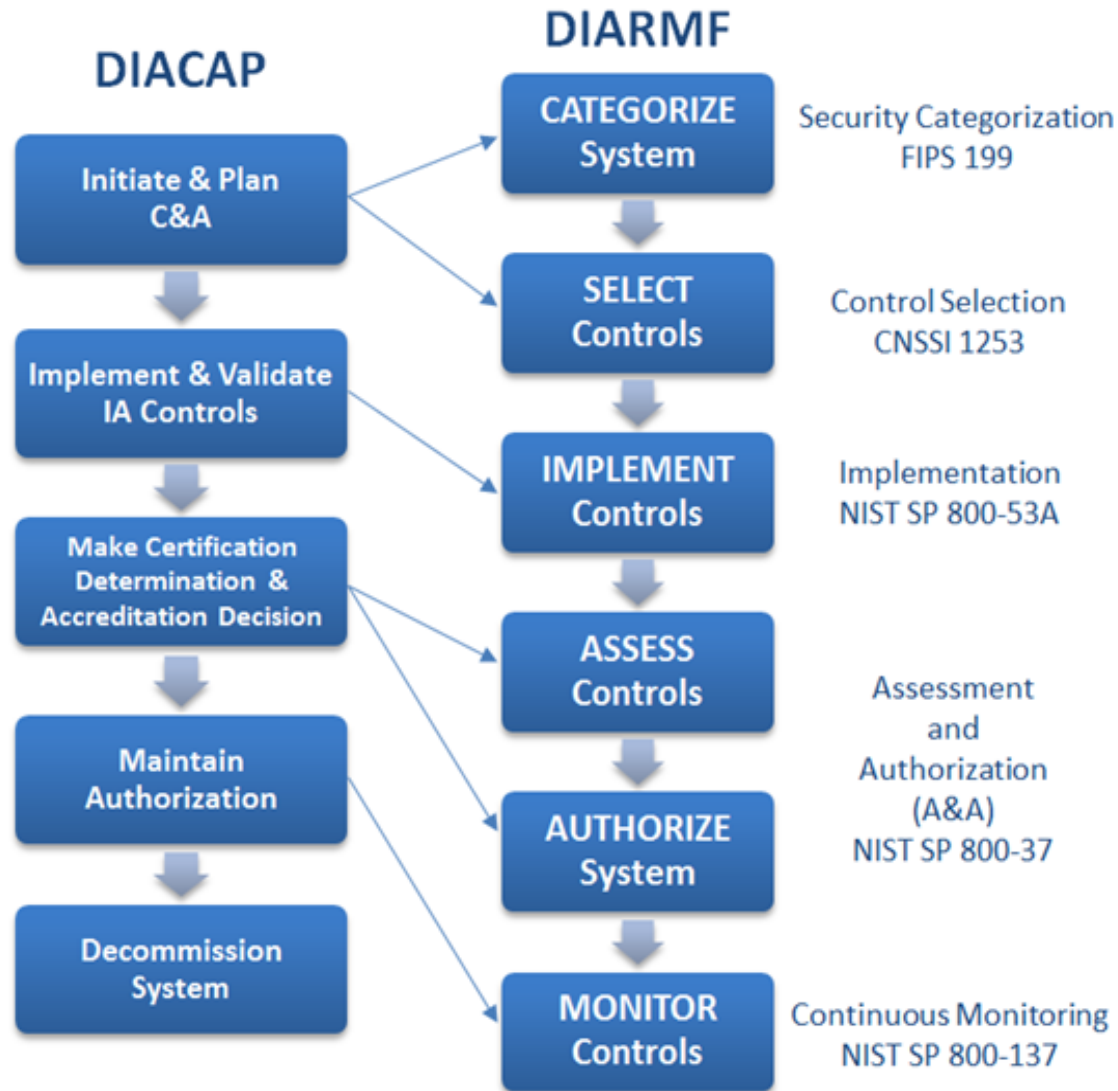
Requirement 11 Regularly test security systems and processes.

PCI DDS 2.0



- ▶ 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.
- ▶ Intrusion Detection and Security Analysis • Chapter 7 309
- ▶ 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.

DIACAP



DCSS-2 System State Changes

- ▶ 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.

