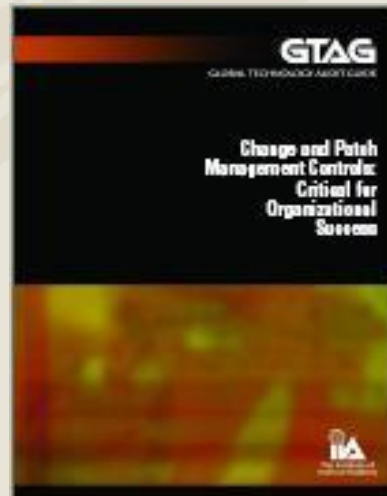


Change and Patch Management Controls Critical for Organizational Success



Global Technology Auditing Guide 2

What This Guide Covers

- Why IT change and patch management controls are foundational to a healthy IT environment
- How IT change and patch management controls help manage IT risks and costs
- What works and doesn't work in practice
- Describes sources of change and the likely impact on business objectives

What This Guide Covers

- Compares effective change management (best practices) and ineffective change management (red flag indicators)
- Discusses the Top Five Steps to reduce IT change related risks
- Provides assessment tool and describes what internal auditors should do

In Summary: This GTAG provides a working knowledge of IT change management processes and risks

Understanding IT Change Management

- Business requirements drive the need for a high degree of IT uptime (availability) while regulatory requirements such as Sarbanes-Oxley drive the need for controls to ensure the confidentiality and integrity of information
- Stable and managed IT production environments require that changes be implemented in a predictable and repeatable manner
- IT personnel implementing changes must follow a controlled process that is defined, monitored and enforced
- Preventative controls (segregation of duties) and detective controls (supervisory) are needed in combination

Change Management Maturity

Effectiveness

Organization controls the changes:

Changes control the organization:

1 - Reactive

- **Over 50% of time spent on unplanned work**
- Chaotic environment; lots of fire fighting
- MTTR is very long; poor service levels
- Can only scale by throwing people at the problem

2 - Using Honor System

- **35-50% of time spent on unplanned work**
- Some technology deployed
- You have the right vision but no accountability
- Server-to-admin ratio is way too low
- IT costs are too high
- Process subverted by talking to the "right" people

3 - Closed-Loop Process

- **15-35% of time spent on unplanned work**
- Some ticketing / workflow system in place
- Changes documented and approved
- Change success rate is high
- Service levels are good & becoming world class
- Server-to-admin ratio is good, but not BoB
- IT costs are improving
- Security incidents down

4 - Continuously Improving

- **<5% of time spent on unplanned work**
- Change success rate is very high
- Service levels are world class
- IT operating costs are under control
- Can scale IT capacity rapidly with marginal increases in IT costs
- Change review and learning processes are in place
- Able to increase capacity in a cost-effective way

Reactive

Using The Honor System

Closed-Loop Change Mgt

Continuously Improving

Why Audit Change Controls?

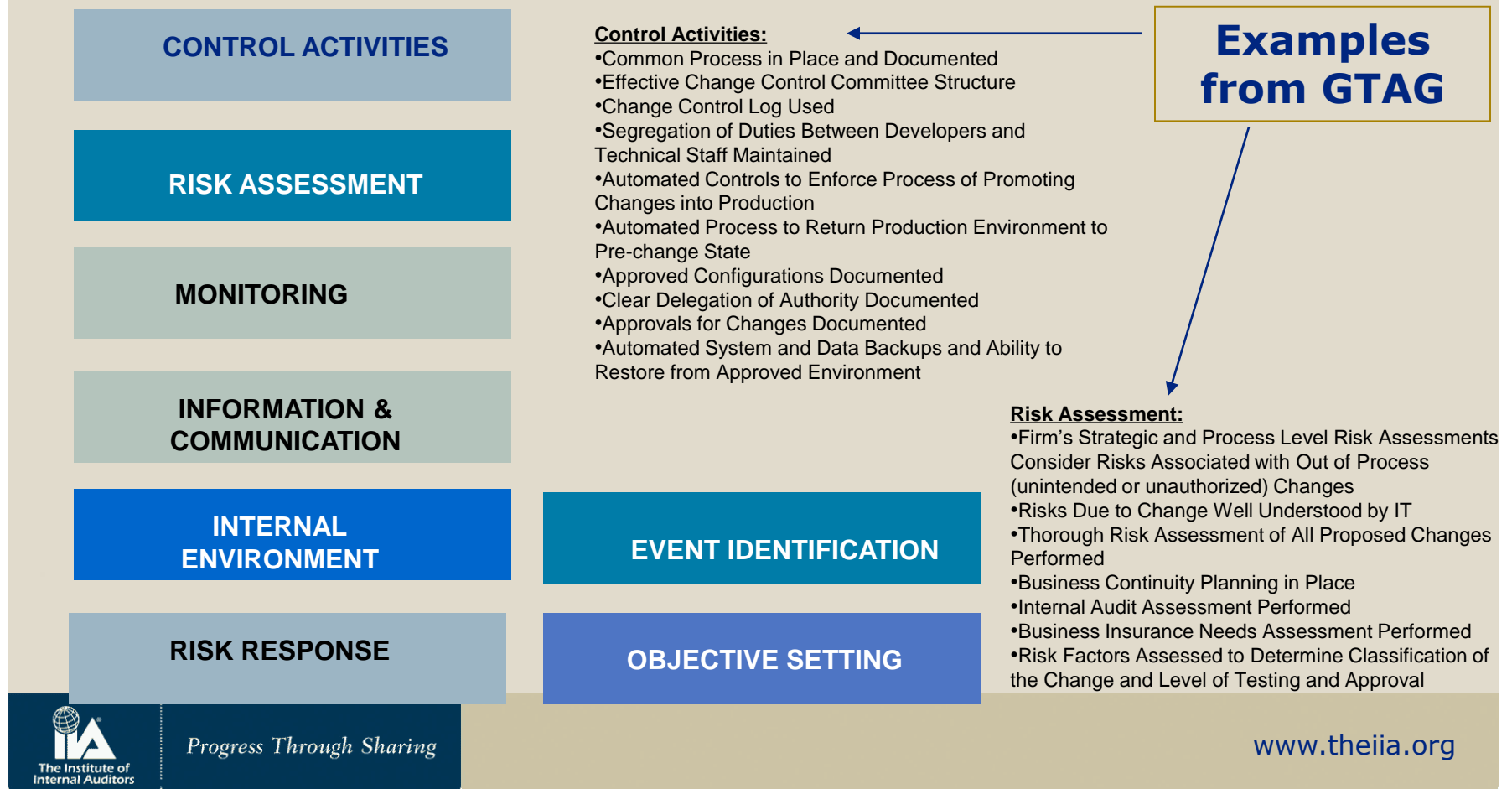
- Increased regulatory requirements around IT controls
 - Increased focus from Audit Committee and Senior Management
 - Internal auditors responsible for providing IT controls assurance
- Technology is everywhere -- 80% of an organization's IP is in electronic form
 - All business decisions result in at least one IT change. When changes are not controlled, they can impact the entire organization
 - According to analysts, 80% of all outages are due to change,
- Consequently, CAEs cannot delegate responsibility for IT change management to IT auditors

Benefits of Good Change and Patch Management Processes

- Spend more time on new development work to advance business goals and objectives
- Reallocate IT staff resources to deliver new capabilities versus “putting out fires”
- Spend less time on unplanned IT work
- Less IT downtime
- Ability to install critical patches with minimal disruption

Assessing Change & Patch Management Processes - 2

- COSO ERM Model For Change & Patch Management



Roles and Responsibilities

- Board of Directors / Governing Body
 - Audit Committee – consider organization's ability to manage IT risks by monitoring deficiencies in critical processes such as change management
- Management – Define, approve, implement and execute IT change management processes
 - Roles vary for developers, operators, testers, approvers, and others
- Auditor
 - Internal Auditors – provide assurance to management
 - External Auditors – independent assessment to determine reliance on controls for preparing financial statements and complying with Sarbanes-Oxley