Introduction to Automated Controls

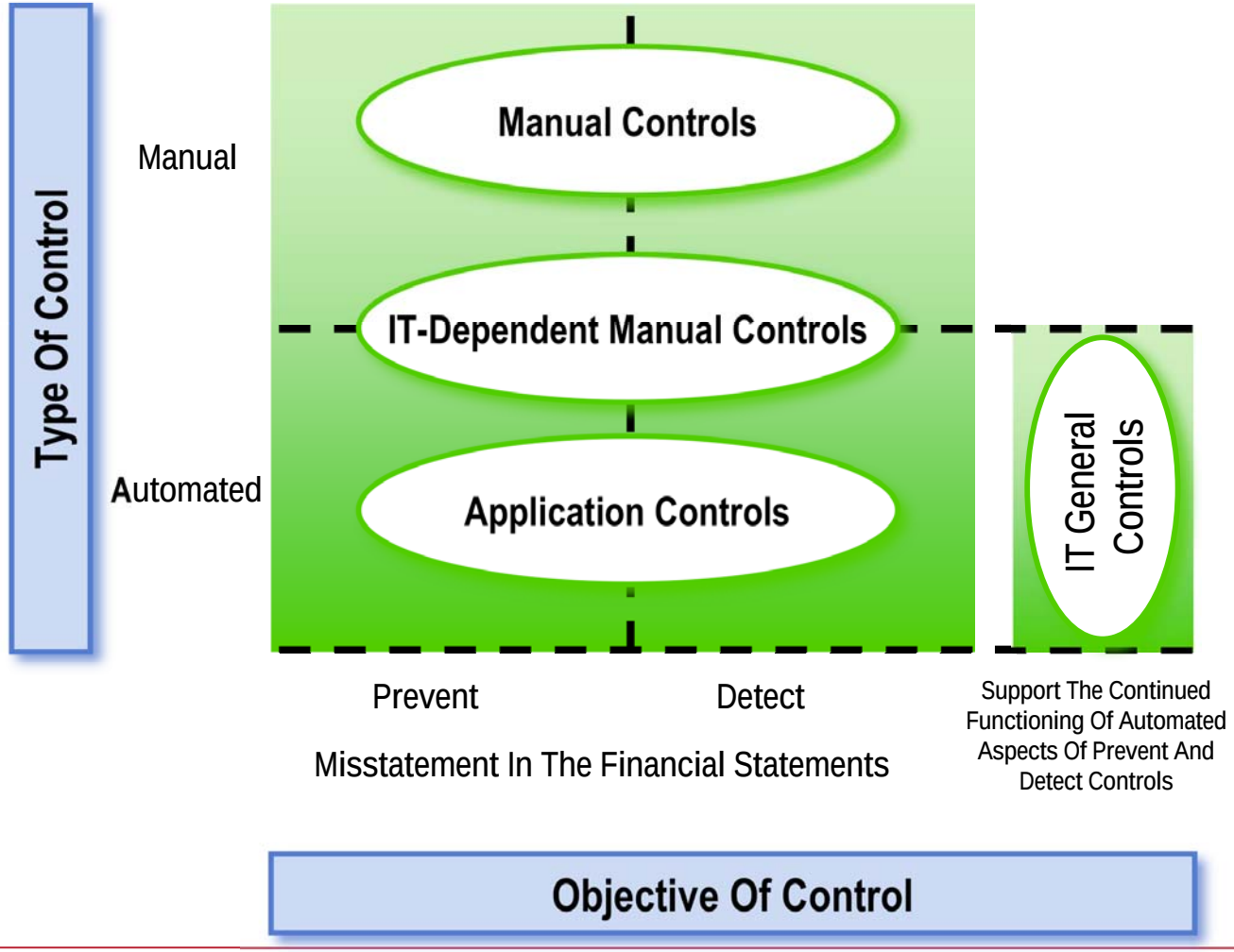
Matthew Hatch, Oliver Petri

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Agenda

- Defining Automated Controls
- The Value of Automated Controls
- Common Testing Approaches
- The Concept of 'Benchmarking‘
- Questions / Comments

Categories of Controls



Inherent vs. Configurable Controls

- Inherent processing and controls
  - Built into the application
  - Examples: DR = CR, system delivered reports, etc.
- Configurable controls
  - Customized and can be disabled or set up to operate in different ways
  - Examples: three-way matching, auto-accounting
- Programmed controls (custom coded)
  - Custom functionality

Types of Application Controls

- Edit Checks
- Validations
- Calculations
- Interfaces
- Authorizations

Automated Controls Are Dependable

- If it works once, it works consistently (assuming IT General Controls are operating effectively)
- However: Might behave differently for different classes of transactions

Testing Approach

- Test of Design
  - Inquiry and observation procedures to understand the design of the control. Typically includes evidencing the system configurations that enforce the logic of the application control.
    - Example: Reviewing the Oracle Set-up or Workflow settings that drive approval limits for purchases.
- Test of Effectiveness
  - Examination of one transaction to confirm the operational effectiveness of the control.

Questions / Discussion:

- When is a ‘negative test’ appropriate?
- What additional procedures are appropriate when a application control is set up differently in different areas of the business (set of books or company code specific configurations).

Testing Examples

- Inspect configuration
  - Inspect 2/3/4-way match configuration
  - Inspect tolerance levels configured
- Re-performance via a walkthrough of each significant flow of transactions
  - Demonstrate the operating effectiveness of the control via positive and negative confirmation
- Inspect the authorizations and reperform controls to confirm the operating effectiveness
  - Inspect privileges assigned to a sample of users
- Determine how overrides are possible throughout testing and how they are monitored

Test Of One

- IT General Controls must be effective
- ITGC must cover automated controls (e.g., configuration changes)
- If configuration is made on lower level (customer, supplier, item, etc.) then one sample might not be sufficient
  - Example: Tolerances are set up uniquely for each set of books / company code.

Overall Cost Of Compliance

- Implement once (cost depending on type of control)
- Lower cost in operation of control
  - Less dependence on humans
  - Fewer errors
  - Less paper
- Control assessment usually more efficient
  - Test of One
  - Benchmarking

Change Control Concerns

- Ability to make code changes is not limited to programmers
- End users have ability to change configuration settings
- Standard change management process not followed for configuration settings
- Security access to make configuration changes is not restricted
- Override of the control by super users or system/database administrators

Overrides

- Segregation of duties
- Workarounds and back-door threats

Example: SAP 3-way match can often be overridden by the user when a purchase order is completed. The user can 'uncheck' the 'GR/IR' indicator eliminating the requirement for matching to the receipt of goods.

Benchmarking

- Benchmarking is the ability to roll forward prior conclusions on application control effectiveness based on the ability to demonstrate a static and controlled environment.
- Historically very difficult to achieve due to complexities within the ERP environment and the dynamic (regularly changing) nature.
- GRC Software packages now making true benchmarking feasible.

Question / Discussion: Does benchmarking become irrelevant if continuous monitoring (via GRC tools, etc.) can be achieved?

Benchmark Testing Approach

- Monitoring
- Rotational Testing

Case Study

Expanding Reliance on Automated Controls

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Objective

- Identification of unmitigated risks or redundant controls
- Identify additional automated controls
- Increase the efficiency of testing the controls

Rationale

- Once implemented, application controls are significantly cheaper to operate.
- Application controls are more consistent and secure than manual controls.
- Application controls are very often the only controls within an automated process.
- It could be more efficient to rely on application controls rather than doing substantive testing.

Process

1. Meetings with Process Owners to understand the process
2. Working session to determine control set and testing approach
3. Draft implementation plan
4. Confirm changes and discuss the plan to implement

Result

- Identified controls that were already implemented and contributed to the mitigation of risk
- Implemented new application controls that reduced the need for manual controls
- Used benchmarking for some application controls to increase the efficiency of the controls assessment

Control mix **prior** to review – 90% manual, 10% automated

Control mix **after** review – 50% manual, 50% automated

Questions?

ISACA
Serving IT Governance Professionals
San Francisco Chapter