G12:
Implementation to Business Value

An ISO 27001 Journey at McKesson

Back to Business

Agenda

- ✓ Who is McKesson?
- ✓ Building the Business Case
- ✓ Strategy and Framework
- ✓ Tools and Maintenance
- ✓ Awareness Campaign
- ✓ Questions

Who is McKesson?

- *Largest* healthcare services company in the world
  - Fortune 15 – $112 billion in revenues (FY11)
  - More than 36,000 employees dedicated to healthcare ▼

- *Oldest* U.S. healthcare company
  - Established 1833 – 178 years driving innovation in healthcare

- *Only* company offering solutions at every point of care

- *Deep* clinical, IT and process expertise

Who is McKesson?

A Diverse Business

- Creating Value at Every Point of Care

Manufacturers
400 Pharmaceutical
2,000 Medical-Surgical
950 Consumer Product

Healthcare Providers
200,000 Physicians
10,000 Long-Term Care Facilities
5,000 Hospitals
(including VA and DoD)
750 Home Care Agencies

McKESSON
Empowering Healthcare

Health Plans
600 Payor Organizations
(Public and Private)

Consumers
25 Million Covered Lives

Agenda

- ✓ Who is McKesson?
- ✓ **Building the Business Case**
- ✓ Strategy and Framework
- ✓ Tools and Maintenance
- ✓ Awareness Campaign
- ✓ Questions

Building the Business Case

External ISO Drivers

Building the Business Case
Internal ISO Drivers

This profession is about more than technology solutions (widgets) for security 'problems'…

…it is about is understanding technology risks in business context.

Certifications should be chosen to manage **business risk**.

Building the Business Case

Describing What is ISO/IEC 27001?

- International Standardization Organization (ISO)/ International Electro technical Commission (IEC)
  - Created ISO 9000 standard : quality manufacturing
- ISO 27001 standard: Minimum baseline for an Information Security Program and supporting Controls

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

McKesson Corporation
One Post Street, Fl 7
San Francisco
California
94104
USA

Holds Certificate No: IS 565574

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

The operation of an information security management system by the Business Technology Solutions (BTS) Department it processes, transmits, and stores for internal and external partners for the BTS core systems and services. The core BTS systems within the scope of the ISMS are classified by the Pharma Disaster Recovery Program as "Tier 1" systems. These systems support the US Pharmaceutical ("Pharma") Order-to-Cash ("OTC") and Procure-to-Pay ("PTP") processes in accordance with the SOA dated 7 September 2010.

For and on behalf of BSI:

VP Regulatory Affairs, BSI Group America Inc.

Originally Registered: 12/07/2010 Latest Issue: 12/07/2010 Expiry Date: 12/06/2013

Page: 1 of 2

Building the Business Case

Articulating Benefits

Benefits

- Market differentiator
- Supports ongoing customer audit requests
- Demonstrates information security discipline
- Is a risk-based approach to compliance
- Matures security programs

Certified Once … Accepted Globally

Challenges

- Formalizes processes, documentation and external audit activities
- Requires investments
- Maintain and improve continuously … ongoing

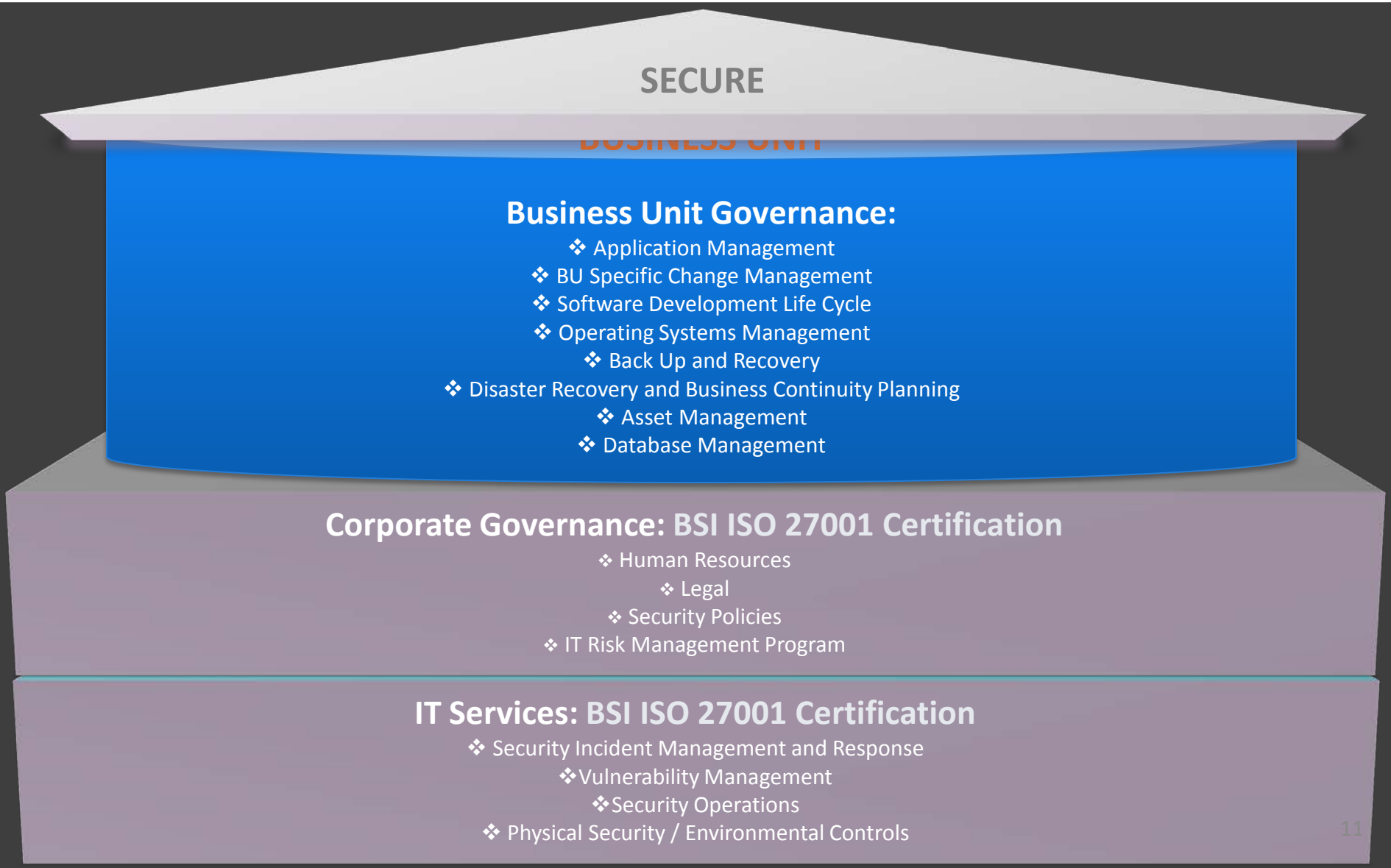
Once you have it – you need to keep it!

Agenda

- ✓ Who is McKesson?
- ✓ Building the Business Case
- ✓ **Strategy and Framework**
- ✓ Tools and Maintenance
- ✓ Awareness Campaign
- ✓ Questions

Strategy and Framework

Scoping – the Key to Success



Strategy and Framework

ISMS - Documented Components

Key documents of an Information Security Management System (ISMS) include the following:

ISMS Policy

ISMS Manual

ISMS Scope Statement

ISMS Leadership

ISMS Terms and Conditions

Statement of Applicability (SOA)

Risk Assessment Methodology

Risk Assessment Report

Internal Audit Report

Strategy and Framework

ISMS - Documented Components

ISMS Policy

- Summarizes the overall goals and objectives of the ISMS and it's purpose within the organization

ISMS Manual

- Refers to or consists of organizational policies, procedures, standards, and guidelines, which at minimum, include the following:
  - Document and records control
  - Management responsibility
  - Internal Audit
  - Management review of the ISMS
  - Metrics and success criteria
  - ISMS Improvement
  - Identification of Legislation

Strategy and Framework

ISMS - Documented Components

ISMS Scope Statement

- Details the scope of the ISMS or in other words, “What is being certified”
- Collaborate with senior leadership and applicable system, data, and process owners
- Specify out of scope areas
- If applicable, point to other ISO 27001 certifications
- Length of the overall readiness process depends on the size of the scope

ISMS Leadership

- Defines the roles and responsibilities of the leadership team that will own and manage the ISMS

ISMS Terms and Definitions

- Provides definitions on Company or ISMS specific terminology or acronyms

Strategy and Framework

ISMS - Documented Components

Risk Assessment Methodology

- Structured approach to risk management. Key areas should include the following:
  - Risk assessment planning and scoping
  - Threat and vulnerability assessment
  - Evaluating business risk (impact, likelihood, residual risk, etc.)
  - Risk prioritization
  - Risk mitigation

Statement of Applicability (SOA)

- The SOA lists the 133 ISO 27001 control standards
- These should be reviewed by appropriate parties to determine applicability
- Control activities/references should be documented for all “included” standards
- The control owner and areas affected should be documented for each control

Strategy and Framework

ISMS - Documented Components

Risk Assessment Report

- Based on the guidelines and procedures specified within the methodology document
- Scope based on what was stated in the ISMS Scope Statement document
- Residual risk calculation:

Risk	Risk Description	Inherent Impact	Likelihood	Risk Impact Score	Inherent Impact	Existing Controls	Mgmt/ Control Level	Residual Risk Rating Level	Decision
Data Center Outage	Outages occur within the data center facilities, which may result in the unavailability of critical applications, systems, and services, and ultimately result in financial, operational, and reputational loss for the Company.	5	2	10	Significant	A.9.1.4, A.14	2	4	Accept

- Note any gaps identified and the associated risk treatment plan

Internal Audit

- Performed by independent body (internal or external)
- Perform test of design procedures
- Leverage work performed by other risk management or compliance initiatives
- Final product includes an audit report with associated gaps and risk treatment plans
- Testing results and evidence inputted in a GRC tool

Strategy and Framework

Communication

Communication

- Send communication to provide awareness and understanding of the ISMS components
- ISMS should be managed over time through steering committee meetings or equivalent

Strategy and Framework

Stage 1 Expectations

Stage 1 Audit

- High-level in nature
- Focus is to ensure that there are no glaring gaps in the ISMS
- ISO 27001 auditor primarily focuses on the ISMS documents
- Operational areas may be sampled and reviewed at a high level
- Ensure version control and dates are documented
- Management review should be performed prior to the audit
- Internal audit review should be performed prior to the audit
- Identified gaps will not appear on the final report if managed

Strategy and Framework

Stage 2 Expectations

Stage 2 Audit

- Verifies that all ISMS requirements have been satisfied
- Detailed review of the ISMS documentation
- Interviews are conducted with system, data, and/or process owners
- Test evidence will be requested for a sample of controls
  - May include a sample of 1 control instance or multiple instances
- Status meeting is held at the end of each day to discuss findings
  - Major non-conformities require a re-audit prior to certification
- Ensure that all participants and related teams are aware of the ISMS

Agenda

- ✓ Who is McKesson?
- ✓ Building the Business Case
- ✓ Strategy and Framework
- ✓ **Tools and Maintenance**
- ✓ Awareness Campaign
- ✓ Questions

Tools and Maintenance

GRC Tool Benefits

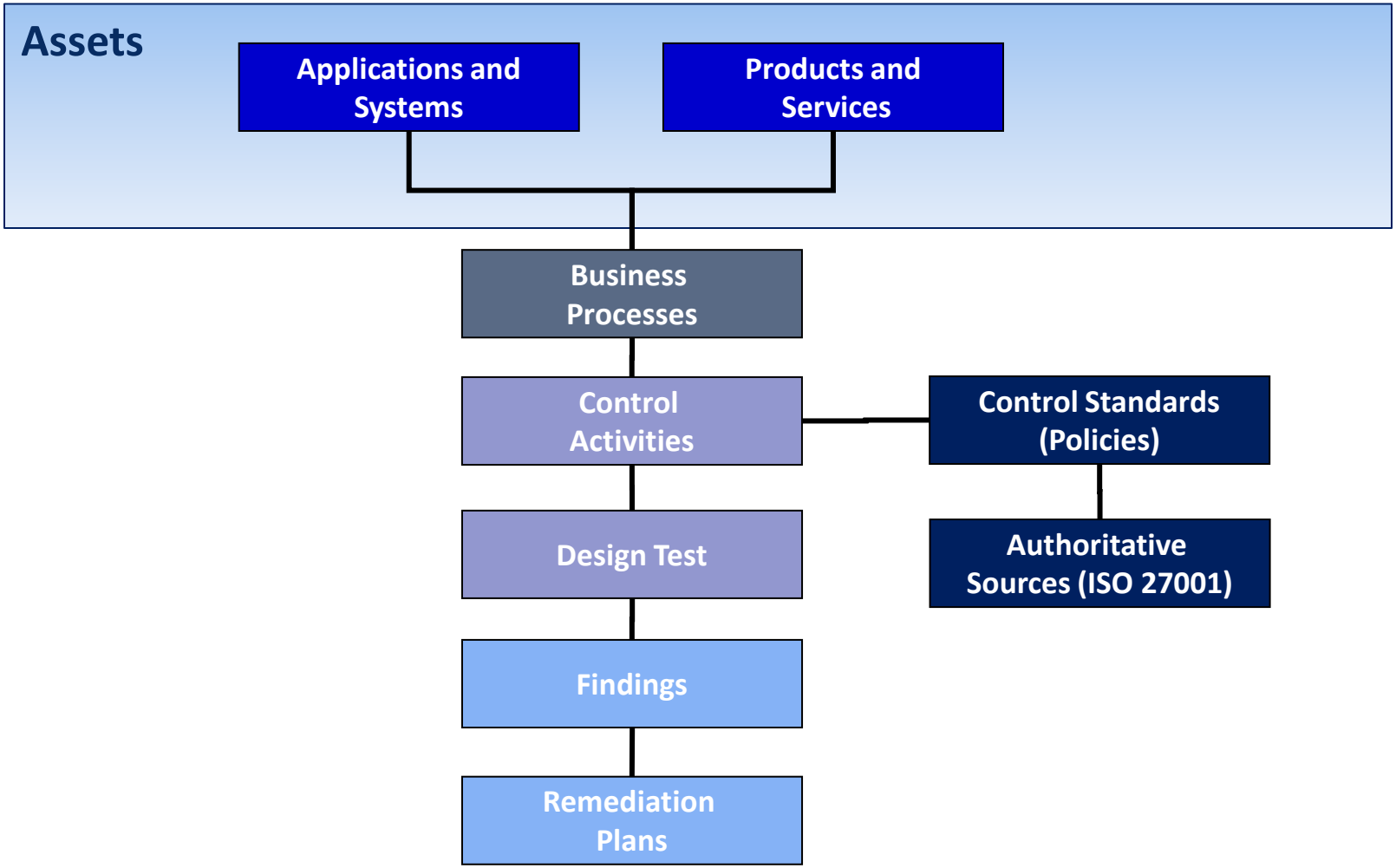
- Improve transparency and consistency
  - Effective management and reporting on IT risk management and compliance efforts
- Streamline our work
  - Leverage integrated content including PCI DSS, ISO 27001, HIPAA, NIST, SOX etc.
  - Identify processes across multiple business units
  - Test centrally to satisfy many regulatory requirements
  - Automation – improved workflow, task management & reporting

Tools and Maintenance
GRC Tool Benefits (Contd.)

- Maintain a centralized repository of controls
  - Test controls and upload evidence
- Process for tracking findings and remediation efforts
- Report compliance at the process as well as policy level
- Sample GRC Vendors - Archer, SAP, Trustwave, Control Path, Compliance 360, Symantec

Tools and Maintenance

Overview of Compliance Management



Tools and Maintenance

ISO Controls Testing

- Work with resource(s) to create processes and controls in Archer

- Link controls to ISO authoritative source
- Link controls to policies

- Validate findings with process owners, senior management
- Track Remediation Plans to completion

- Identify dedicated resource(s) in BU
- Train resource(s) in Archer

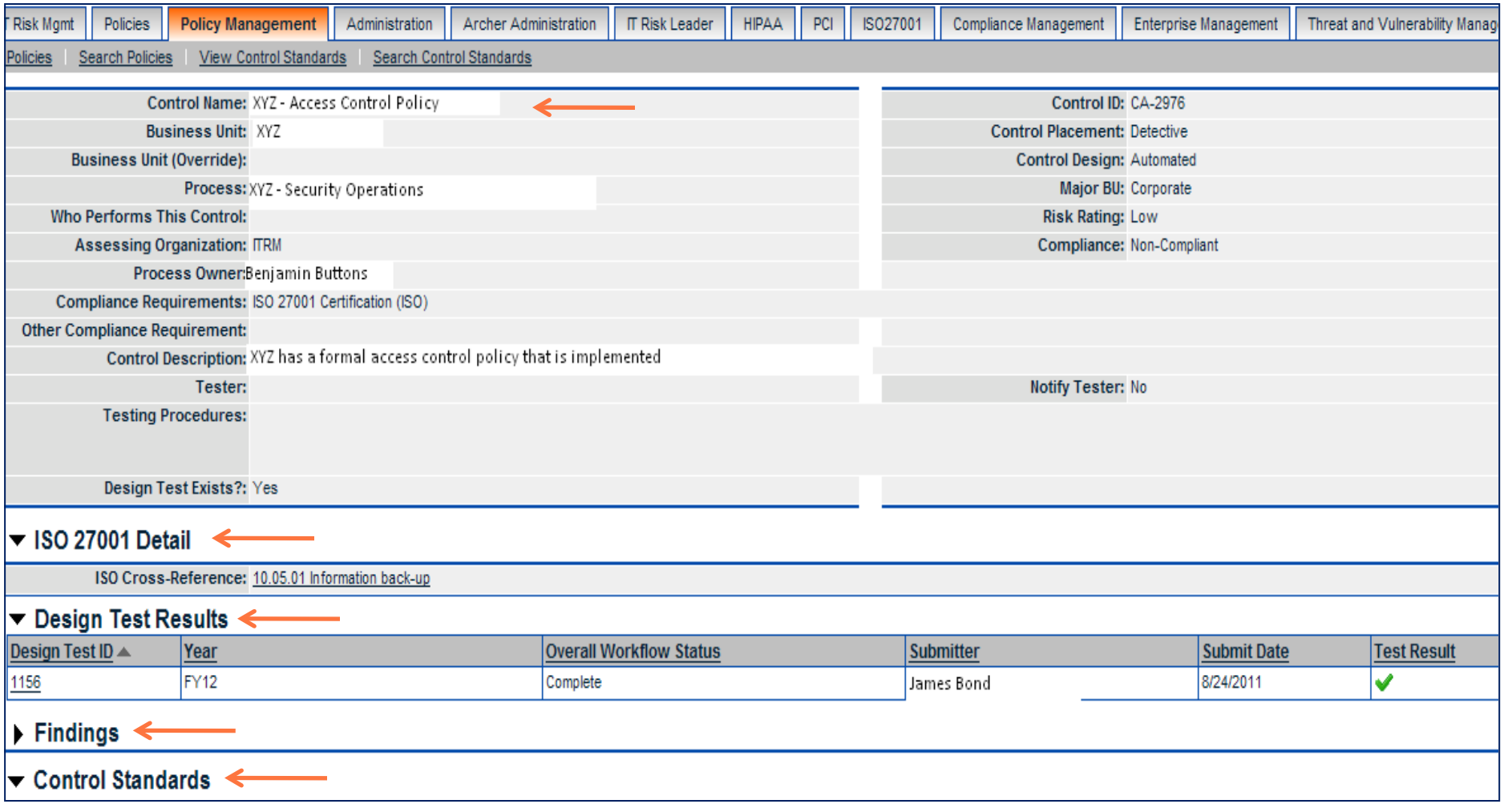
- Rationalize ISO controls with existing controls (PCI, SOX, etc)

- Test controls and attach evidence

24

Tools and Maintenance

Demo – Control Activity



Tools and Maintenance

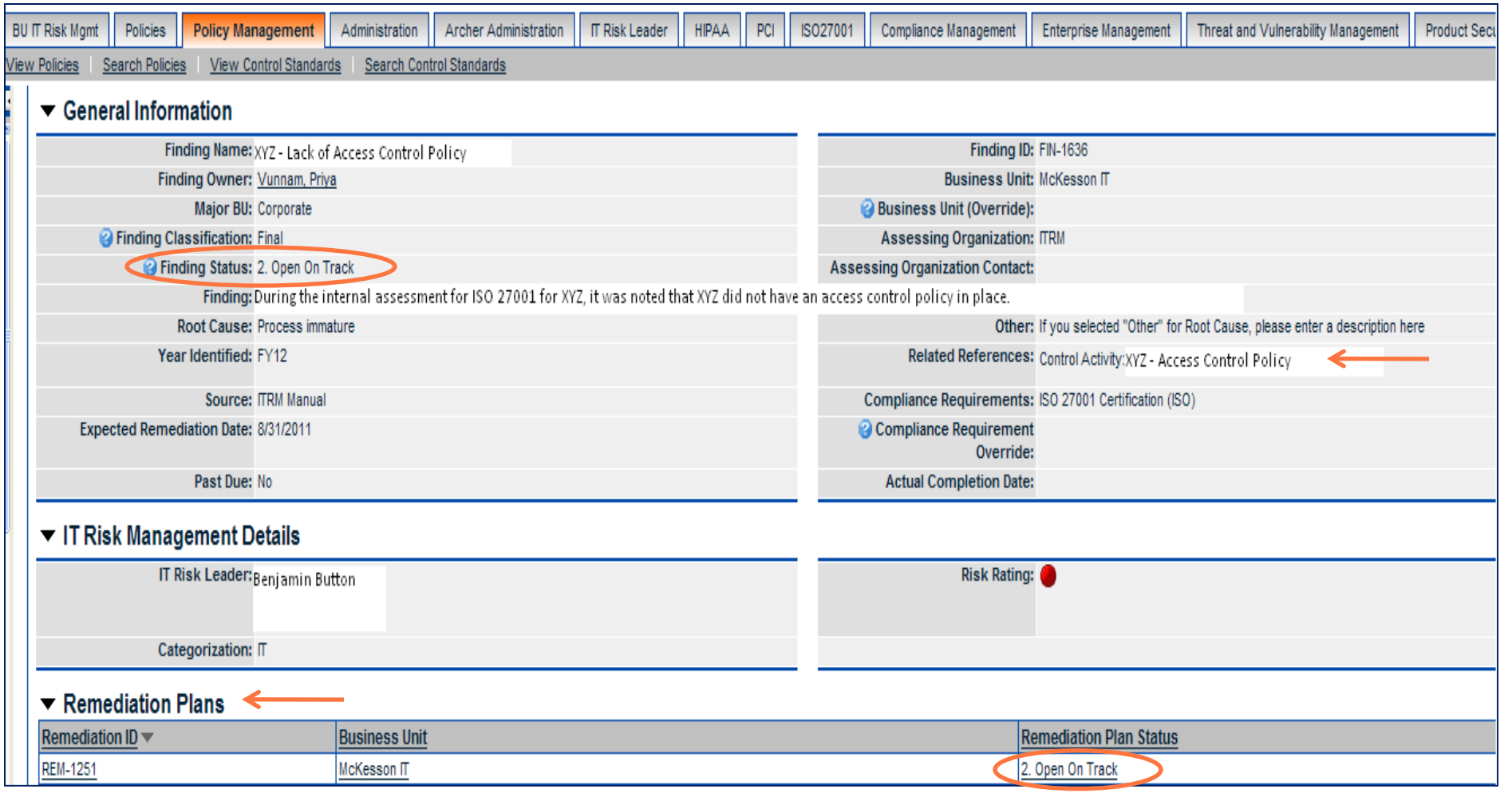
Demo – Control Standard

Control Standards
08/25/2011

Standard Name ▲	Standard ID	Statement	Authoritative Sources
Acceptance Testing	ATCS-828	All significant modifications, major enhancements and new systems must be acceptance tested by the appropriate users prior to installation of the software in production. The user acceptance plan will include tests of all major functions, processes, and interfacing systems. Testing procedures must be properly documented on the change request forms.	COBIT 4.1 Acquire and Implement AI 07.07 Final Acceptance Test FFIEC Information Systems Standards FFIEC IT Management (2004) ITCI38 IT Controls Implementation - Testing of new technology Payment Card Industry PCI DSS v1.2 06.3.1 Secure Systems and Applications - Testing ISO/IEC 27002:2005(E) 10.0 Communications and Operations Management 10.03 System planning and acceptance 10.03.02 System acceptance 12.0 Information Systems Acquisition, Development and Maintenance 12.04 Security of system files 12.04.01 Control of operational software

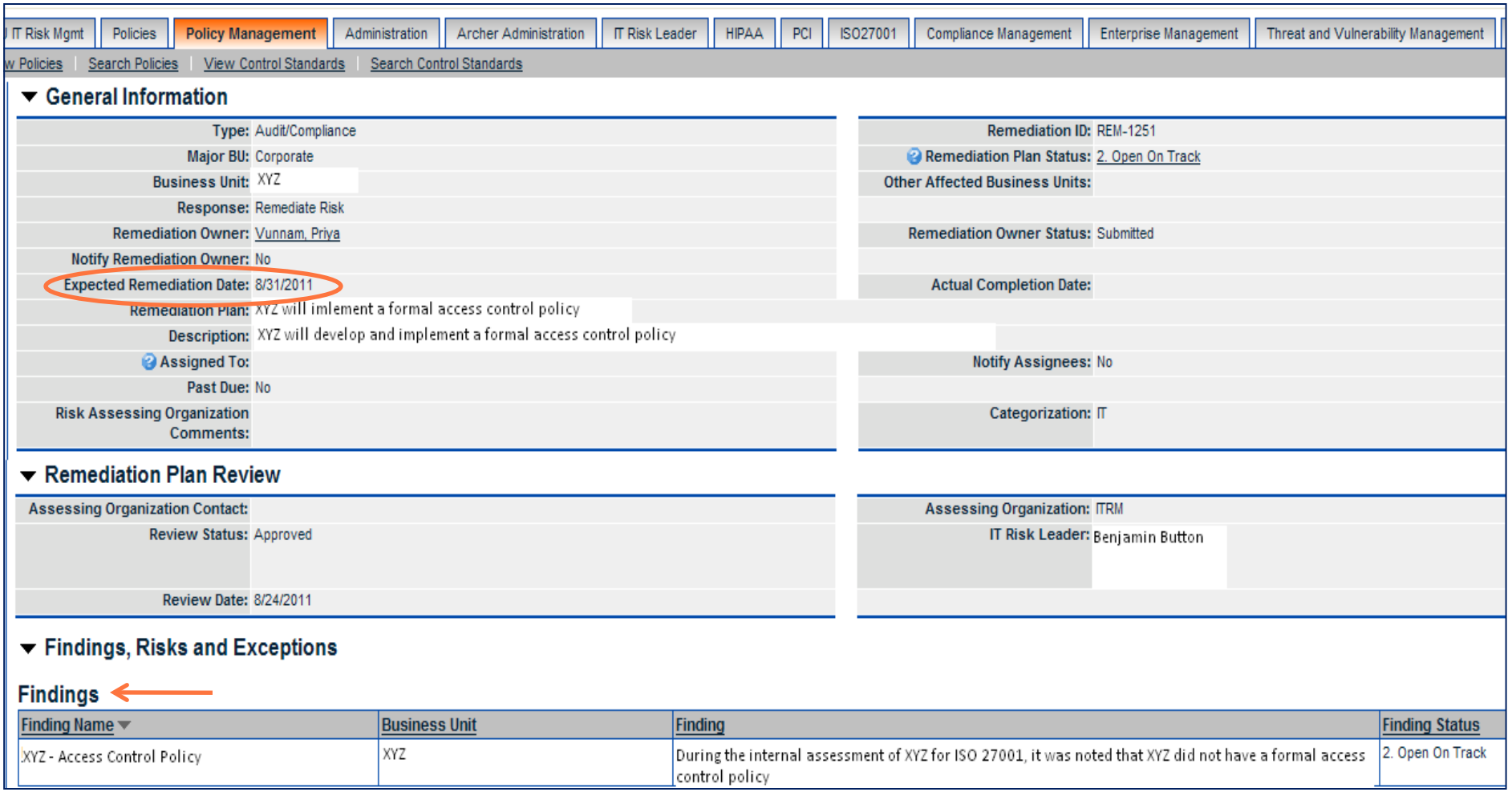
Tools and Maintenance

Demo - Finding



Tools and Maintenance

Demo – Remediation Plan



IT Risk Mgmt | Policies | **Policy Management** | Administration | Archer Administration | IT Risk Leader | HIPAA | PCI | ISO27001 | Compliance Management | Enterprise Management | Threat and Vulnerability Management

w Policies | Search Policies | View Control Standards | Search Control Standards

General Information

Type:	Audit/Compliance	Remediation ID:	REM-1251
Major BU:	Corporate	Remediation Plan Status:	2. Open On Track
Business Unit:	XYZ	Other Affected Business Units:	
Response:	Remediate Risk		
Remediation Owner:	Vunnam, Priya	Remediation Owner Status:	Submitted
Notify Remediation Owner:	No		
Expected Remediation Date:	8/31/2011	Actual Completion Date:	
Remediation Plan:	XYZ will imlement a formal access control policy		
Description:	XYZ will develop and implement a formal access control policy		
Assigned To:		Notify Assignees:	No
Past Due:	No		
Risk Assessing Organization Comments:		Categorization:	IT

Remediation Plan Review

Assessing Organization Contact:		Assessing Organization:	ITRM
Review Status:	Approved	IT Risk Leader:	Benjamin Button
Review Date:	8/24/2011		

Findings, Risks and Exceptions

Findings

Finding Name	Business Unit	Finding	Finding Status
XYZ - Access Control Policy	XYZ	During the internal assessment of XYZ for ISO 27001, it was noted that XYZ did not have a formal access control policy	2. Open On Track

Tools and Maintenance

Are we ready???

- Control activities (CAs) created
- CAs linked to ISO reqs
- Test results and evidence
- Report of all open findings with expected remediation date
- SOA updated with Archer CA number

Tools and Maintenance

Obtain Certification

CONGRATULATIONS!!! You are now ISO 27001 certified

Tools and Maintenance

ISO Certification Continuous Maintenance

- Automated custom-built notifications for maintenance activities
- Determine the testing period in a fiscal year – test all applicable controls in this period
  - Leverage controls tested for other regulatory requirements (SOX, HIPAA, PCI, etc)
  - Ensure that all the processes specified in the audit schedule are tested
- Track Senior Leadership meetings and maintain minutes in SharePoint/Archer
- Findings- Work with dedicated resource(s) in the BU to track open findings

Tools and Maintenance

Surveillance/Re-Audit Checklist

- ✓ Schedule audit with external auditors
  - Schedule meetings with process owners
- ✓ Update program level documentation
  - ISMS Audit Report
  - ISMS Manual
  - ISMS Policy
  - ISMS Scope
  - Risk Assessment Report
  - Senior leadership Team
  - Statement of Applicability
  - Report of controls testing results

Tools and Maintenance

Surveillance/Re-Audit Checklist (contd.)

- ✓ Internal Assessment
  - Test Results
  - Audit Report
- ✓ Management Approval
  - Get all the program level documentation including the internal audit results approved by a third party

Tools and Maintenance

Surveillance/Re-Audit Checklist (contd.)

- ✓ Schedule post-certification party
- ✓ Design gifts for teammates

Tools and Maintenance

Big Wins

- A single portal for compliance management
  - Integration of disparate processes
  - Compliance of multiple regulations satisfied by single control
  - Real-time status and results dashboards
  - Ease of Maintenance
  - Automated notifications, workflow

- Allows for management of multiple certifications in a centralized repository with a repeatable process

Agenda

- ✓ Who is McKesson?
- ✓ Building the Business Case
- ✓ Strategy and Framework
- ✓ Tools and Maintenance
- ✓ **Awareness Campaign**
- ✓ Questions

Awareness Campaign

Promote the Achievement!

- Do a road show!!!
  - Get statements from sponsors
  - Identify your business supporters
  - Present at sponsorship meetings
  - Get an article on the internal wire
  - Present at conferences ☺
- No one will promote what you do for you - learn to do it yourself
- Be educated in your approach - leverage internal teams like Toastmasters and mentors in the business for feedback on how to present at different levels in order to be the most effective

Questions?