

ITIL, SOX, What's Next?

A Tool and Approach Designed to
Meet Increasing Demands for
Compliance

Andrew C. Galbus
MN HIMSS
Annual Conference 2007

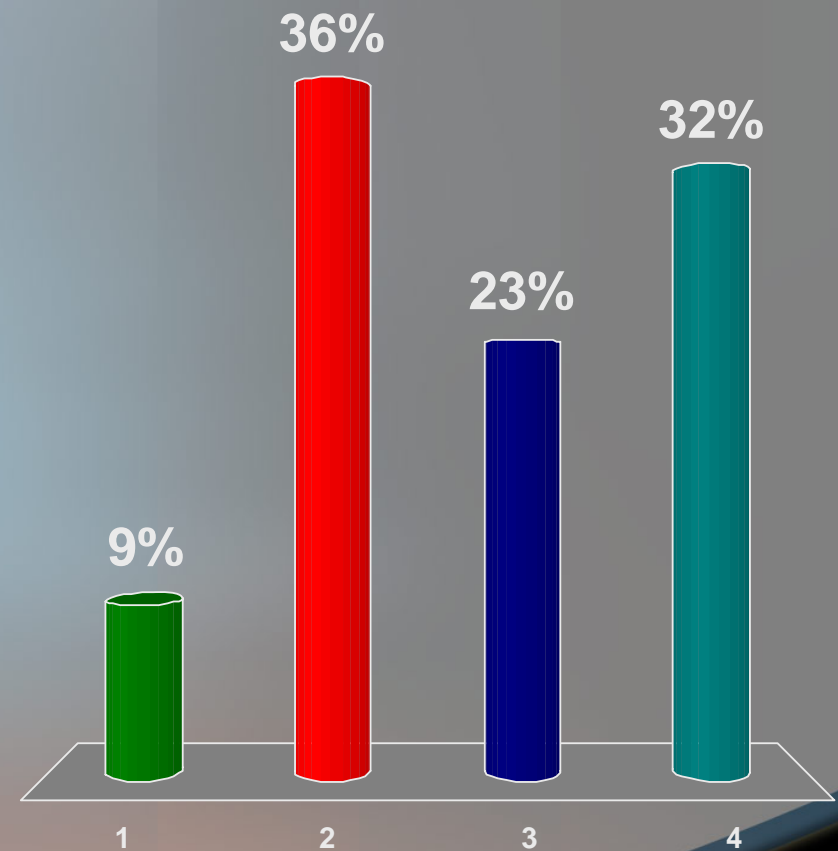
Overview

- ITIL & SOX Knowledge
- Problem Definition
 - ITIL Overview
 - SOX Overview
- Solution
- Lessons Learned
- Any Other Questions?

ITIL & SOX Knowledge

What do you know about ITIL?

1. A lot – we are pursuing it at our organization
2. Somewhat – I am familiar with the basic framework
3. A little – I have heard of it and know a little
4. Never heard of it

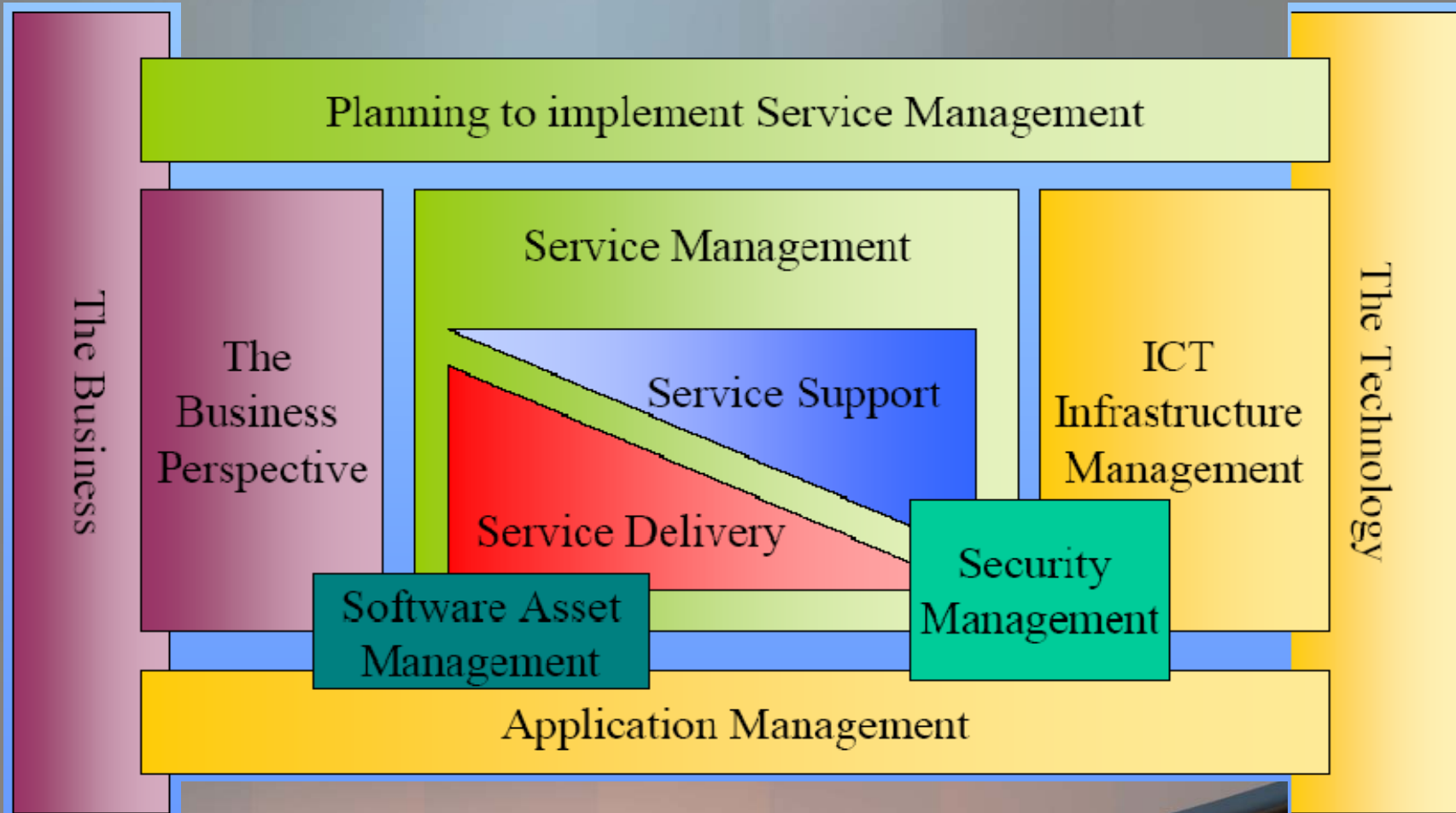


Information Technology Infrastructure Library (ITIL) Primer

ITIL Primer

- ITIL[®] (the IT Infrastructure Library) is the most widely accepted approach to IT service management in the world
 - Cohesive set of best practice from public and private sectors internationally
 - Supported by a comprehensive qualifications scheme, accredited training organizations, and implementation and assessment tools
 - Supported by, the British Standards Institution's standard for IT Service Management
 - A framework, not a methodology
 - itSMF organization helps share the framework – conference in September www.itsmfusion.com

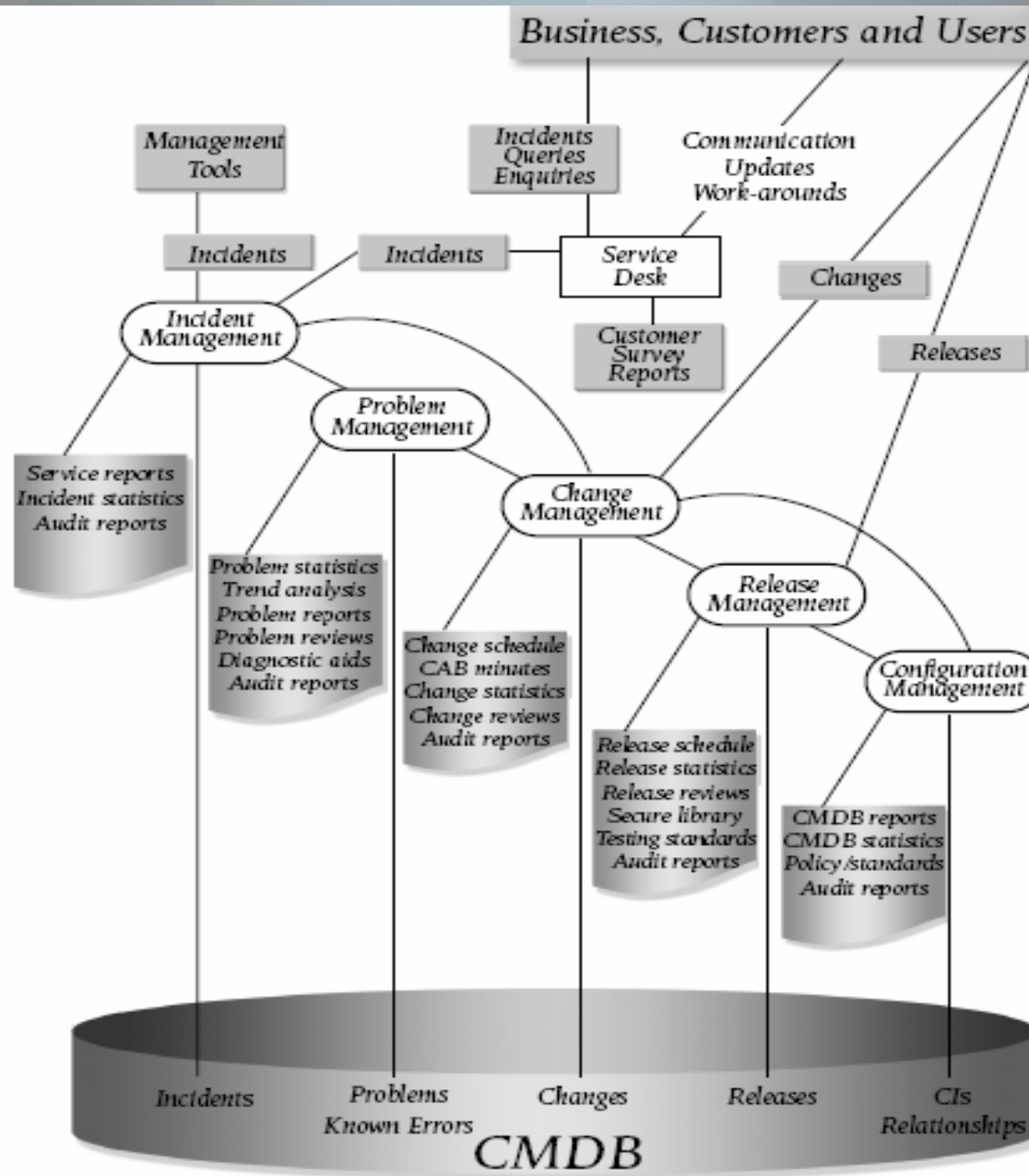
ITIL Primer



ITIL Primer

- Service Management (Support and Delivery of Service) are the largest books in the library with the most attention from organizations
- Service Support is a Book in ITIL with concepts such as:
 - A Service Desk
 - Incident Management
 - Problem Management
 - Change Management
 - Release Management
 - Configuration Management

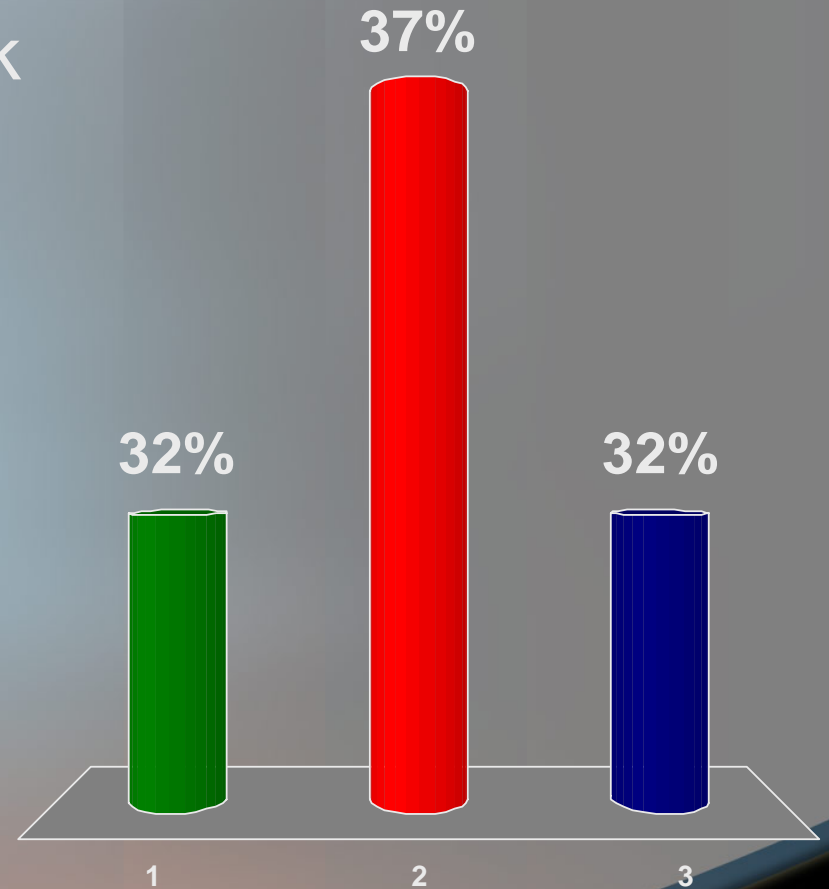
ITIL Primer



ITIL Primer – Quiz Question

Which statement is true?

1. ITIL gives you the framework on how to perform a change management process
2. ITIL evolved from best practices in the United Kingdom before the United States
3. ITIL describes how incident management is linked to change management and release management

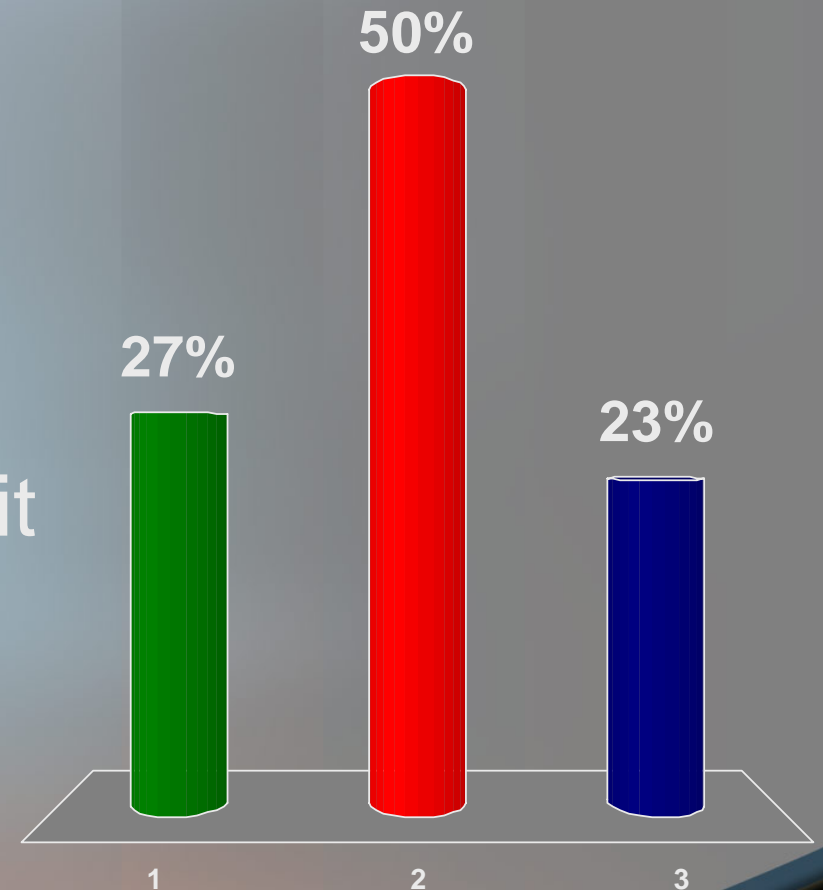


The image features a dark, vertical gradient background transitioning from deep blue at the top to black at the bottom. The letters "SOX" are centered in a white, sans-serif font.

SOX

What do you know about SOX?

1. A lot – SOX means Sarbanes-Oxley Act and our organization is complying with it - I am aware of it
2. A little – I have heard of it and know a little, but not much
3. Never heard of it – but I can now see in question 1, what SOX stands for



Sarbanes Oxley Act - Primer

SOX Primer

A little history...

FEBRUARY 13, 2006 - Blue Cross and Blue Shield of North Carolina said last week that "human error" caused the Social Security numbers of more than 600 of its members to be printed on the mailing labels of envelopes sent to those patients.

Enron grew and grew from 1930's natural gas company as an innovative company. In 2001 the start of the fall with bribery, offshore accounts hiding losses and insider trading. Stock went from \$90 to \$0.30.

OCTOBER 4, 2005 - A judge refused to release the former Tyco International executives L. Dennis Kozlowski and Mark H. Swartz on bail Monday while they appeal their convictions on charges of stealing \$600 million from the company.

FEBRUARY 06, 2006 - Confidential patient data sent to wrong company - for 15 months. Doctors and clinics in the U.S. have been faxing information to an herbal remedy distributor

FEBRUARY 28, 2006 - One employee was fired and three others resigned in connection with the theft in late December of backup computer tapes and disks containing personal information and medical records on about 365,000 hospice and home health care patients from a parked car in Portland, Ore. Some of the data on the tapes was password-protected at the application level, while the rest of the data was stored in proprietary file formats without password protection.

Sarbanes-Oxley (SOX) Legislation

- Legislation sponsored by Senator Paul Sarbanes (D-MD) and Congressman Michael Oxley (R-OH) on July 30, 2002
- Designed to protect investors and provide for increased corporate responsibility
- Requires controls for completeness, timeliness, and accuracy of quarterly financial statements for publicly traded companies
- Primary compliance date: December 31, 2004

SOX Primer

Examples of Internal Controls

Detective

- ✓ Control activities detect errors and requires the user to correct error
- For example
 - Soft coded warning messages
 - Exception reporting
 - Review adjustment reports

Preventive

- ✓ Control activities prevent errors from occurring
- For example,
 - Hard coded error messages
 - Min/max range requirements
 - System access limitations

Manual

- ✓ Control activities require initiation by system or process user
- For example,
 - Report analysis
 - Manual reconciliation

Automated

- ✓ Control activities automatically occur due to system functionality or programming
- For example,
 - Required fields
 - Interface / conversion programs

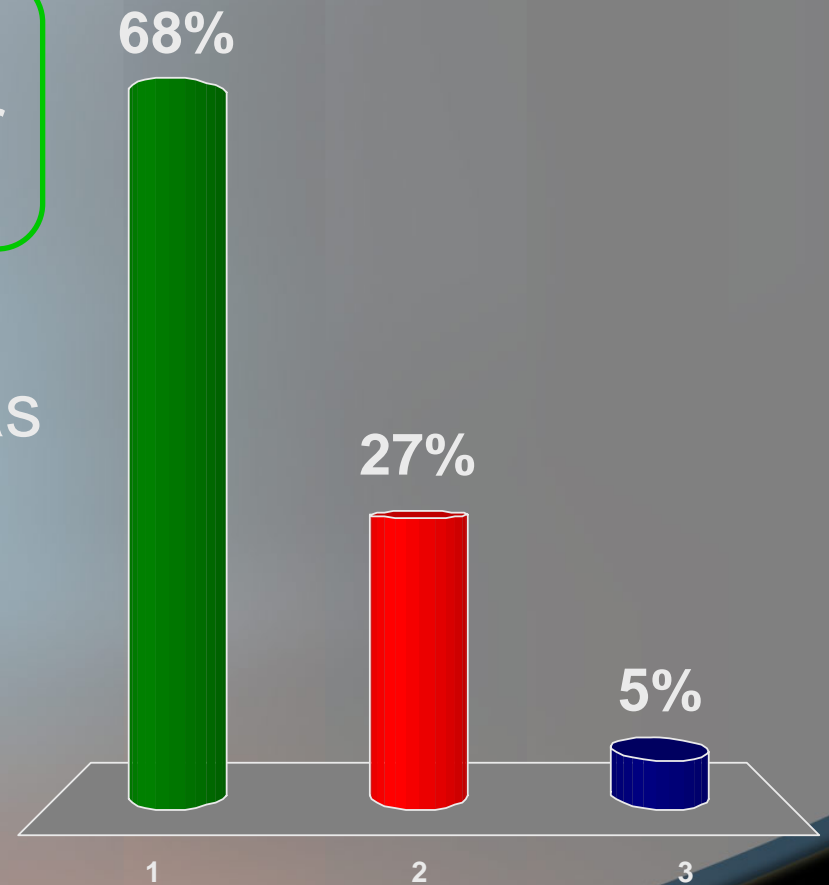
Types of IT General Controls

- System development life cycle (implementation, changes, replacement)
- Managing system performance and capacity
- System security
- Data interface controls
- Computing facility environmental controls
- Backup and recovery
- Managing operations

SOX Primer – Quiz Question

Which statement is true?

1. SOX requires companies to have controls to protect their financials
2. SOX is required for not-for-profit organizations as well as for-profit ones
3. ITIL describes how incident management is linked to change management and release management



Problem Definition

Problem Definition

At Mayo Clinic we have many regulatory bodies asking us to comply:

- Audit: We are pursuing controls like Sarbanes Oxley for our Financials (sections 302 and 404)
- The College of American Pathologist (CAP) regulates our Laboratory practice including IT systems
- Internally our IT organization has created policies for processes such as change management
- HIPAA requires our IT systems have security, protection of patient identifiers, etc.
- Joint Commission (JCAHO) require us to have policies and procedures for Information Management

Problem: How can we proactively accommodate these needs rather than react to the increased demands for compliance?

The Solution

Approach and Tool

Approach

- A small group of four met for several weeks analyzing the existing known requirements regarding one topic – IT Change Management (Each person had a unique perspective, background, skill to contribute)
- A simple tool was developed that would cross reference each requirement (spreadsheet)
- Each tab represented each requirement (SOX, ITIL, IT policy, HIPAA, JCAHO)
- The policy was selected as the “anchor” from which to compare each regulation to

Approach

- Feedback was gathered on each of the requirements independently
- The group met to discuss each other's feedback
- The policy was revised and presented to committees for approval based upon feedback
- The tool is used for future changing regulatory requirements

Approach – View of Tool

Microsoft Excel - CM Matrix.xls

File Edit View Insert Format Tools Data Window Help Adobe PDF Type a question for help

	B	C	D	F	G	H	I
1	Change Management Policy [Version 8/1/2006]	CM Policy 06-28-2000	SOX (ICE)	Mayo Security	JCAHO	CAP/C LIA	
2							
3							
4	Policies must be in place to allow IT to identify, prepare and implement changes as efficiently and effectively as possible. By adhering to the following policies and principles, IT will have the greatest opportunity to accomplish the Change Management objectives.	Pur1, Pur2					
5	Change Management is essential to managing risk introduced by making changes to information technology components. While managed changes are accelerated, they include three change, record	Pur3, Pur4, Pur5					
6							
7	Mayo Rochester Information Technology changes will be managed using change management processes and guidelines to ensure systems integrity and acceptable risks while supporting Mayo's business and practice needs.	Pol1			IM 2.20.1	GEN.43 077	
8	Each work unit shall establish, document and implement Change Management Procedures that includes: change identification, change analysis, change development, and implementation controls.	P1, Req 5-1	12.1.1.1 12.1.4.2 12.1.4.6 12.3.1.1			GEN.43 011	
9	The Change Management process will address how urgent changes will be conducted. Change Management will be applied to in-house developed and vended applications.	P1, Req 1-2, 3-3, 3-4, POL3	12.1.1.1 12.1.4.2				
10	Changes affecting the characteristics or configuration of Mayo's production environment are subject to the Change Management Process and will be managed in accordance with designated processes and guidelines. (e.g., software, system parameters, operating system, database, hardware, network)	P1, P2	12.1.1.1				
11	This Change Management Policy is the responsibility of the Information Technology Coordinating Council (ITCC).	Pol2					

One version of our change management policy

Cross-reference to an older version of policy

Cross-references to other policies / mandates

CM Policy / CM 2000 / HIPAA / SOX (ICE) / Mayo Security / CAP-CLIA / JACHO

Approach – View of Tool

The screenshot shows a Microsoft Excel spreadsheet titled "Microsoft Excel - CM Matrix 04-20-07.xls". The spreadsheet contains a table with columns A, B, C, and D. The table is organized into sections: "Change Management Policy [Version March 2007]", "1.0 PURPOSE", and "2.0 SCOPE". The "2.0 SCOPE" section is further divided into three sub-sections: "2.0 (1)", "2.0 (2)", and "2.0 (3)". The "2.0 (3)" sub-section contains a list of items: "request process", "change analysis", "development milestone review / approval", "testing", "business acceptance, and", and "implementation controls". The "ICE 2007" cell is highlighted in green. The "Cross References" text is written in blue, with arrows pointing to the "ICE 2007" cell and the "request process", "change analysis", "development milestone review / approval", "testing", "business acceptance, and", and "implementation controls" items. The bottom of the spreadsheet shows a row of tabs: "CM Proposed", "ICE 2007", "CM 2006", "CM 2000", "HIPAA", "ICE 2006", "Mayo Security", and "CAP-CLIA".

	A	B	C	D
1				
2	Change Management Policy [Version March 2007]			ICE 2007
3				
4	1.0 PURPOSE			
5	1.0 (1)	Change Management is essential to managing risk introduced by making changes to information technology components. While managing risk, the rate of change must also be accelerated to meet business demands for IT solutions. Risks include threats to system integrity, outages, unauthorized change, recoverability, security, etc.		
6	1.0 (2)	Mayo Rochester Information Technology changes will be managed and communicated using change management processes to ensure systems integrity and acceptable risks while supporting Mayo's business and practice needs.		
7	2.0 SCOPE			
8	2.0 (1)	Changes affecting the characteristics or configuration of Mayo's production environment are subject to the Change Management Policy. • software • system parameters • operating system • database • hardware • network	12.1.1	
9	2.0 (2)	Change Management will be applied to in-house developed and vended applications; and will address how urgent changes will be conducted.	12.1.1 12.1.4.2	
10	2.0 (3)	Each work unit will establish, document and implement Change Management Procedures that addresses: • request process, • change analysis, • development milestone review / approval, • testing, • business acceptance, and • implementation controls.	12.1.1.2 12.1.2.3 12.1.4.1	

Approach – View of Tool

Microsoft Excel - CM Matrix.xls		File Edit View Insert Format Tools Data Window Help Adobe PDF				Type a question for help
	B	F	G	H	I	J
1	Change Management Policy [Version 06-28-2000]	LB	AG	ES	BB	Comments
15	Scheduling of changes will be based upon managing the risk they present to both the production environment and the business objectives of Mayo.	x	x	x	X	Scheduling here is expanded to include authorization and prioritization in CM 2006. We need more of this type of specificity CES The 2006 policy should include the scheduling comments. BB
16	To allow for IT-wide scheduling and proper communication, change information will be provided in a timely manner.	x	x	x	X	"timely manner" can prove to be a moving target and should be explicitly stated. Then and only then can IT-wide scheduling be appropriater managed. CES
17	Continuous improvement practices will be employed to	x	x	x	X	
18				x	X	Support for standard tools noted ACG Do we need to narrow down what that "set" of management tools needs to be? CES
20	Change Identification					
21	A method to identify requested changes, problems and their current priority/status shall be maintained.	x	x	x	X	Should we try to be consistnet in our wording, i.e., "shall" vs "will" be? CES I think it should be consistant. BB
22	A process will be established to recognize, implement and track emergency changes.	x	x	x	x	
23	Analysis					
24	Users should participate in the development of documented system requirements.	x	x	x	x	While this is sometimes outside the control of the IT team, I think we should begin to move twoards "requiring" user participation. SOX requires user acceptance and approval. See SOX 12.1.1.2; 12.1.2.1; 12.1.2.2.; 12.1.5.1.CES I gree with Estelle. If we stay with softer language, the task may be neglected. BB
	A documented method is used to evaluate risks and benefits (both business & technical) associated with a proposed change.	x	x	x	x	Observation that many statements mention risk. I wonder if there is a cross reference that should note all items dealing with risk. ICE asks for risk in the impact

Gathering input is critical – independent and then as a group

Approach: Draft Policy

Change Management Policy Mayo Clinic- Rochester: Information Technology

1.0 PURPOSE

Change Management is essential to managing risk introduced by making changes to information technology components. While managing risk, the rate of change must also be accelerated to meet business demands for IT solutions. Risks include threats to system integrity, outages, unauthorized change, recoverability, security, etc.

Mayo Rochester Information Technology changes will be managed and communicated using change management processes to ensure systems integrity and acceptable risks while supporting Mayo's business and practice needs.

2.0 SCOPE

Changes affecting the characteristics or configuration of Mayo's production environment are subject to the Change Management Policy.

- software
- system parameters
- operating system
- database
- hardware
- network

Change Management will be applied to in-house developed and vended applications; and will address how urgent changes will be conducted.

Each work unit will establish, document and implement Change Management Procedures that addresses:

- request process,
- change analysis,
- development milestone review / approval,
- testing,
- business acceptance, and
- implementation controls.

Documented evidence of compliance with these procedures must be created and retained for each change.

Outcome and Benefits

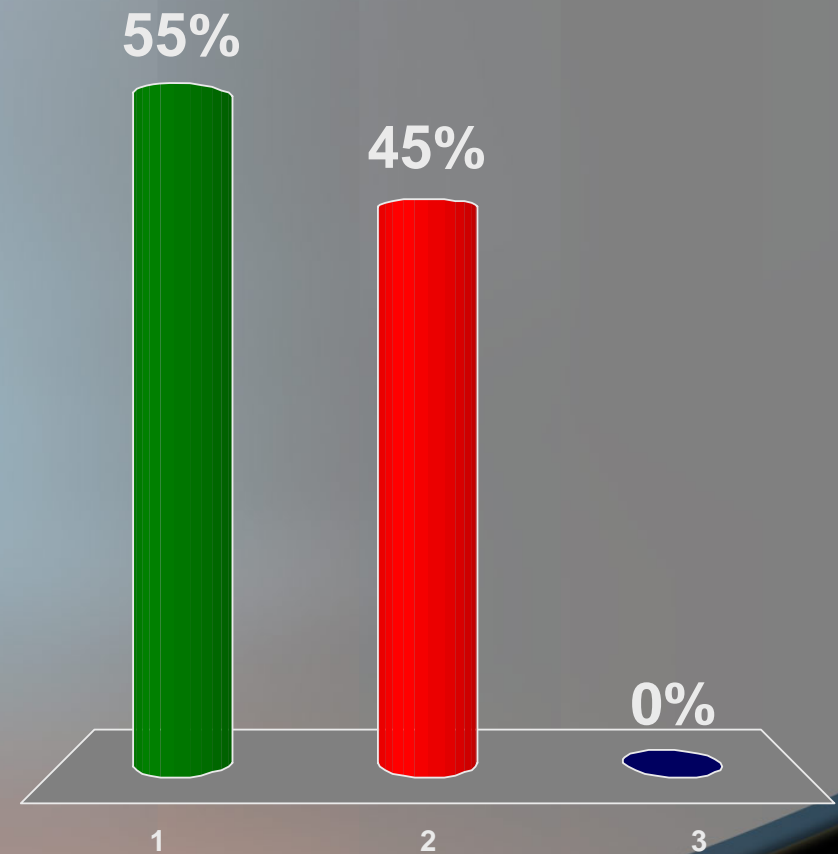
Outcome & Benefits

Other than the policy being revised for multiple purposes...

- The tool can now be re-used for future external organizations asking us to comply
- The tool & approach can be used for other overlapping requirements unrelated
- We can be confident we are not creating separate processes, procedures, guidelines for individual compliance activities unless we really feel we need to

Did this presentation help you?

1. Yes, I now have another approach / tool to help meet increasing compliance needs
2. Somewhat, I learned some ideas that I think I can use
3. No, I knew most of this already



The End
Other Questions?