Happy Life Insurance & IT General Controls

Helping you go public.

Consulting Team: Charles A. Hulebak, Will Bobe, Alivia Coon, Edward Kim

Our consulting team brings over forty years of work experience from backgrounds including technology, innovation, and legal expertise. We seek to align our expertise with the needs of your organizational leadership and objectives.

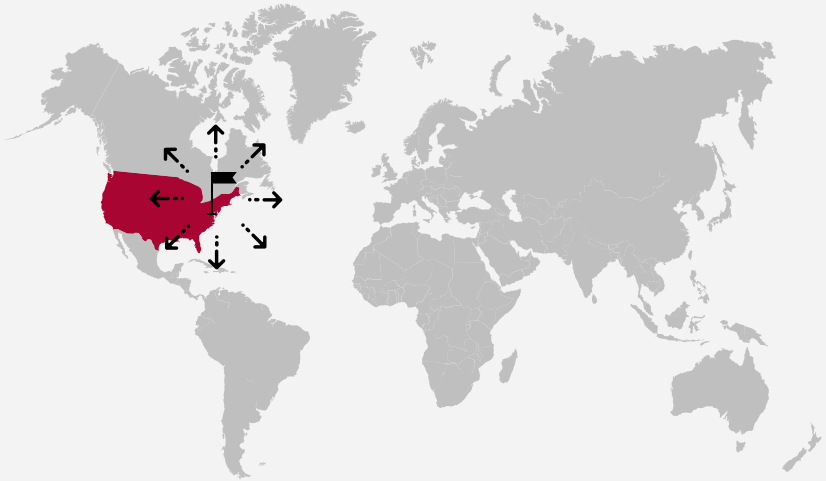
TABLE OF CONTENTS

Introduction and Background

Happy Life Insurance (HLI) is a large, private insurance company based in New York with 34 offices across the country and 40 million members. Serving both the government and the public at large, HLI has experienced 2000% growth in the last two decades and has maintained a great reputation. In order to finance international growth, the company has recently decided to go public.

As HLI embarks on this journey, we are seeking to guide this organization with internal control reporting requirements and compliance concerns through standardized and established information technology frameworks.

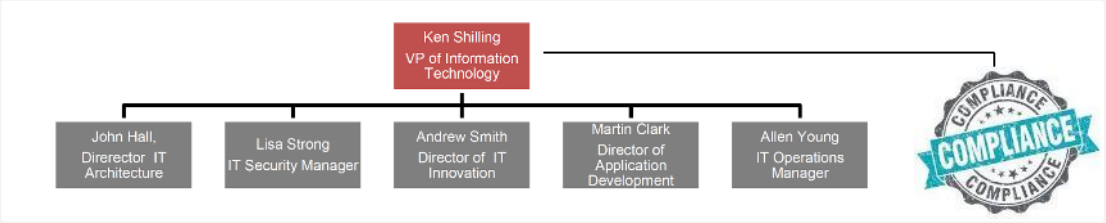
Utilizing ISACA and COBIT framework, HLI will be able to address concerns spanning from security administration, application change control, data backup and recovery, systems development life cycle (SDLC), and others while complying with the Sarbanes-Oxley Act (SOX).



Organizational Outline

HLI's IT organization consists of 150 employees and is led by Ken Shilling, Vice President of Information Technology.
This SAP-driven organization includes the following directors, who will be an integral part of HLI's transition to going public:

- **Internal Application Development group > Martin Clark**
  - Internal solutions and customizations
    - Managers
    - Developers
    - Testers
- **IT Security group > Lisa Strong**
  - Provisioning and monitoring access
    - IT Sec Manager
    - Supervisor
    - End User
    - HR Reps
- **IT Operations group > Allen Young**
  - Data backups, scheduling and processing, incident response
    - Database Ops
    - Help Desk
- **Compliance Team**
  - Managers submit approvals for compliance associated with their unit



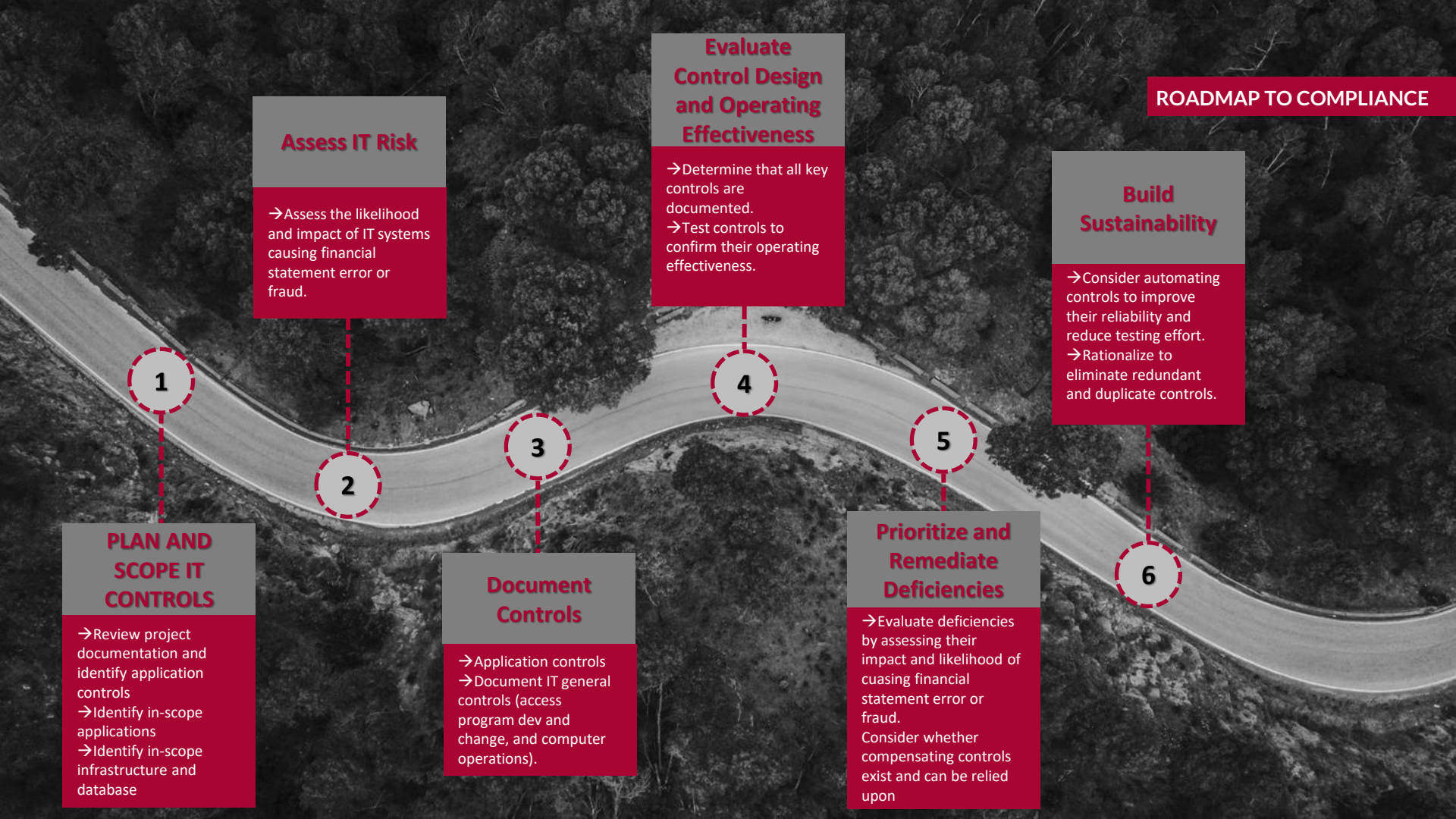
Key Issues and Observations

HLI's consulting team, working in partnership with the HLI's leadership has determined a number of risks, ranging from organizational concerns to change management, logical access management, and operations management.

Through the development of a comprehensive plan, HLI is seeking to address these concerns and others with a robust and dependable IT framework.

Organizational Risks	Reputational risks of a breach HLI is going public Focus on growth rather than security and compliance Sarbanes Oxley Requirements HIPPA / HITECH and patient privacy compliance
Change Management	Application development issues with emergency app changes No application security or secure code during test Approval system issues in app dev management
Logical Access Management	Local representatives have access to comprehensive lists of members All applications accessible to all employees External website connects to internal Oracle database of all customers Weak, user selected passwords and lax enforcement. Credentialing issues Admin access issues
Operations Management	Automating manual systems Manual notifications for de/re access Backup issues

ROADMAP TO COMPLIANCE



1 PLAN AND SCOPE IT CONTROLS

→Review project documentation and identify application controls
→Identify in-scope applications
→Identify in-scope infrastructure and database

2 Assess IT Risk

→Assess the likelihood and impact of IT systems causing financial statement error or fraud.

3 Document Controls

→Application controls
→Document IT general controls (access program dev and change, and computer operations).

4 Evaluate Control Design and Operating Effectiveness

→Determine that all key controls are documented.
→Test controls to confirm their operating effectiveness.

5 Prioritize and Remediate Deficiencies

→Evaluate deficiencies by assessing their impact and likelihood of cuasing financial statement error or fraud.
Consider whether compensating controls exist and can be relied upon

6 Build Sustainability

→Consider automating controls to improve their reliability and reduce testing effort.
→Rationalize to eliminate redundant and duplicate controls.

Common Elements of Enterprises

The general controls will fall into the following processes:

Change Management (“CM”): Primarily concerned with the processes in which changes are made to systems and applications in alignment with SOX and SoD compliance and patient privacy concerns.

Logical Access Management (“LAM”): Primarily concerned with making sure access is limited to the appropriate parties to ensure security of the organization.

Operations Management (“OM”): Primarily concerned with incident and problem handling to ensure documentation for any issues is maintained.

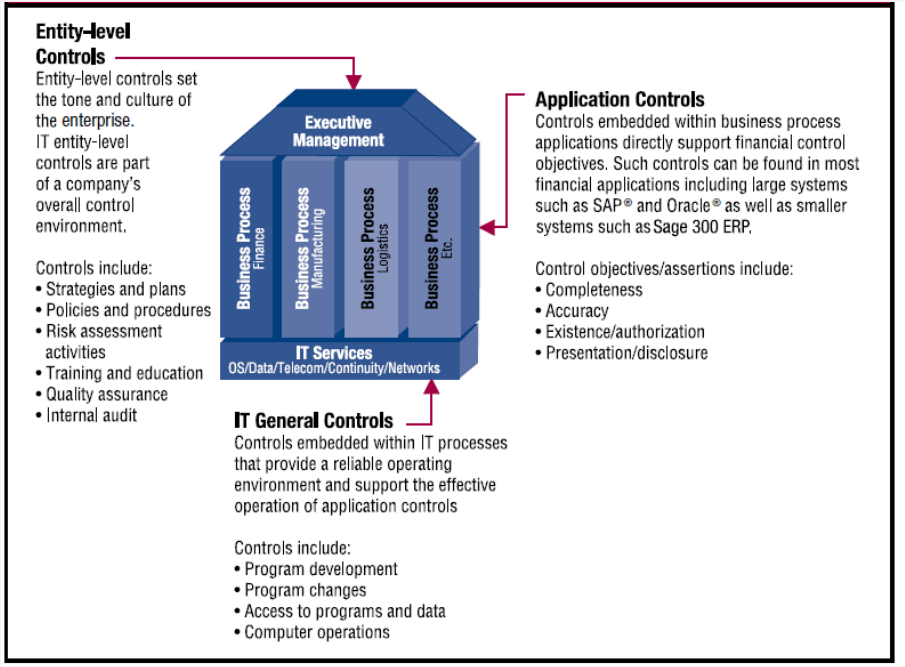


Figure: Common Elements of Enterprises, IT Control Objectives SOX 3rd Edition

Section 2A: Change Management

HLI is developing a plan for managing system and application changes as they prepare for SOX compliance.

This includes authorizing, testing, approving, monitoring, and addressing the segregation of duties (SoD) for changes.

COBIT 5's IT Control Objectives for Sarbanes-Oxley provides guiding framework for change management processes, while ISACA's framework addresses segregation of duties.

HLI should encourage a culture that supports the willingness to change and adapt. This can be accomplished with communication, engagement, and education that covers expectations of future compliance and policies.

FIGURE 4: Five Phases of the Change Management Process

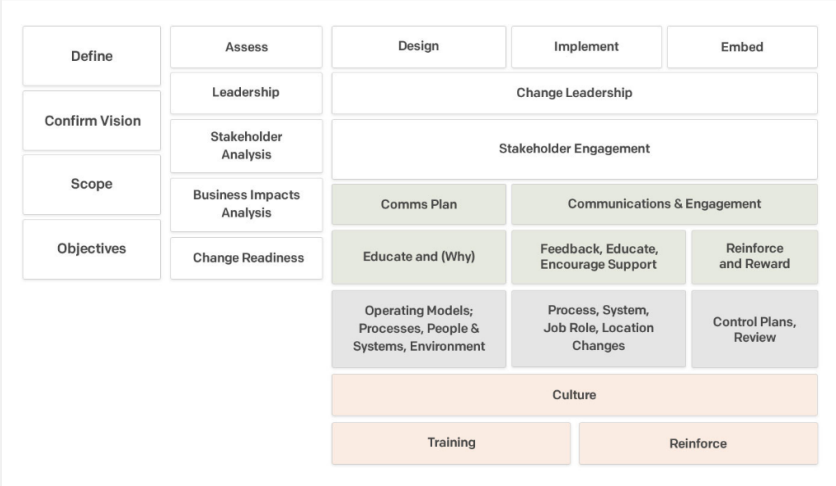


Image: https://daniellock.com/change-management-process/

SOX compliance using SAP, ERP, and GRC

HLI is currently a **SAP (Software, Applications, and Products)** driven organization, with an internal IT group that interfaces with the SAP system. This will make the migration from going private to public much easier for SOX Section 404 compliance.

The SAP platform provides the ability to control processes in a 5-phase process, including evaluation, reporting, documentation, planning, and performing/monitoring.

ERP (Enterprise Resource Planning) business systems provide the ability to continuously monitor controls to ensure that risks are identified and mitigated, compliance is sustained, and business processes are always monitored.

GRC (Governance, Risk, and Compliance) focuses on auditing and risk management, while enabling the ability to comply with standards, laws and requirements. Software may be integrated within the SAP system or independently, focusing on five broad areas including documentation, scope, evaluation, monitoring, and reporting.

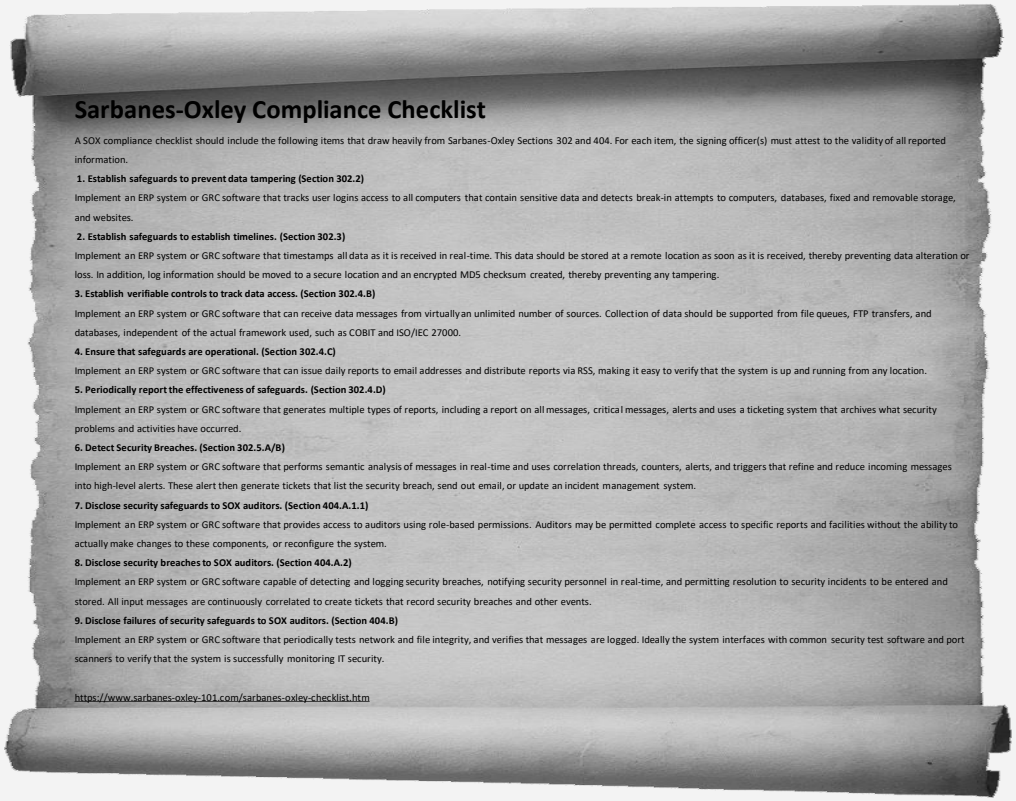
Image: hexaware.com

https://www.sap.com/products/internal-control.html
https://www.ey.com/Publication/vwLUAssets/EY-SAP-GRC-process-control/$FILE/EY-SAP-GRC-process-control.pdf

Identifying and Mitigating Change Risks

There are many existing processes which HLI will need to assess for SOX compliance, as well as procedures and protocols for integrating future changes. HLI can begin this transition by identifying a complete list of these processes and testing a sample of these processes with an established framework, including change authorization, approval, testing, and monitoring.

Furthermore, HLI can develop a mileage chart and testing application chart to identify opportunities to reduce risk for SoD between business and information technology groups.



Sarbanes-Oxley Compliance Checklist

A SOX compliance checklist should include the following items that draw heavily from Sarbanes-Oxley Sections 302 and 404. For each item, the signing officer(s) must attest to the validity of all reported information.

1. Establish safeguards to prevent data tampering (Section 302.2)

Implement an ERP system or GRC software that tracks user logins access to all computers that contain sensitive data and detects break-in attempts to computers, databases, fixed and removable storage, and websites.

2. Establish safeguards to establish timelines. (Section 302.3)

Implement an ERP system or GRC software that timestamps all data as it is received in real-time. This data should be stored at a remote location as soon as it is received, thereby preventing data alteration or loss. In addition, log information should be moved to a secure location and an encrypted MD5 checksum created, thereby preventing any tampering.

3. Establish verifiable controls to track data access. (Section 302.4.B)

Implement an ERP system or GRC software that can receive data messages from virtually an unlimited number of sources. Collection of data should be supported from file queues, FTP transfers, and databases, independent of the actual framework used, such as COBIT and ISO/IEC 27000.

4. Ensure that safeguards are operational. (Section 302.4.C)

Implement an ERP system or GRC software that can issue daily reports to email addresses and distribute reports via RSS, making it easy to verify that the system is up and running from any location.

5. Periodically report the effectiveness of safeguards. (Section 302.4.D)

Implement an ERP system or GRC software that generates multiple types of reports, including a report on all messages, critical messages, alerts and uses a ticketing system that archives what security problems and activities have occurred.

6. Detect Security Breaches. (Section 302.5.A/B)

Implement an ERP system or GRC software that performs semantic analysis of messages in real-time and uses correlation threads, counters, alerts, and triggers that refine and reduce incoming messages into high-level alerts. These alert then generate tickets that list the security breach, send out email, or update an incident management system.

7. Disclose security safeguards to SOX auditors. (Section 404.A.1.1)

Implement an ERP system or GRC software that provides access to auditors using role-based permissions. Auditors may be permitted complete access to specific reports and facilities without the ability to actually make changes to these components, or reconfigure the system.

8. Disclose security breaches to SOX auditors. (Section 404.A.2)

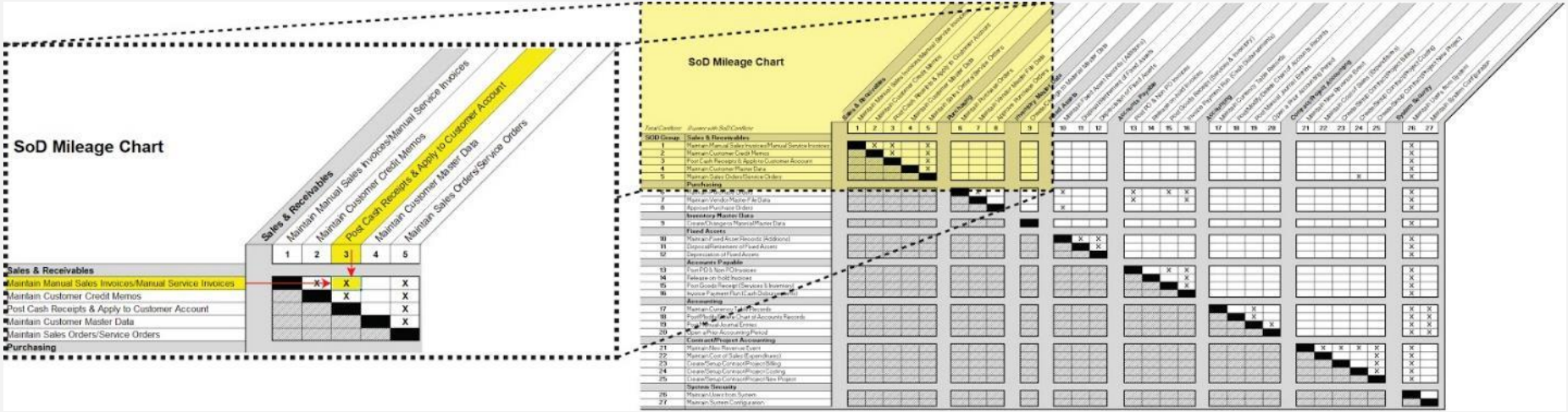
Implement an ERP system or GRC software capable of detecting and logging security breaches, notifying security personnel in real-time, and permitting resolution to security incidents to be entered and stored. All input messages are continuously correlated to create tickets that record security breaches and other events.

9. Disclose failures of security safeguards to SOX auditors. (Section 404.B)

Implement an ERP system or GRC software that periodically tests network and file integrity, and verifies that messages are logged. Ideally the system interfaces with common security test software and port scanners to verify that the system is successfully monitoring IT security.

https://www.sarbanes-oxley-101.com/sarbanes-oxley-checklist.htm

Separation of Duties (SoD) Mileage Chart Implementation



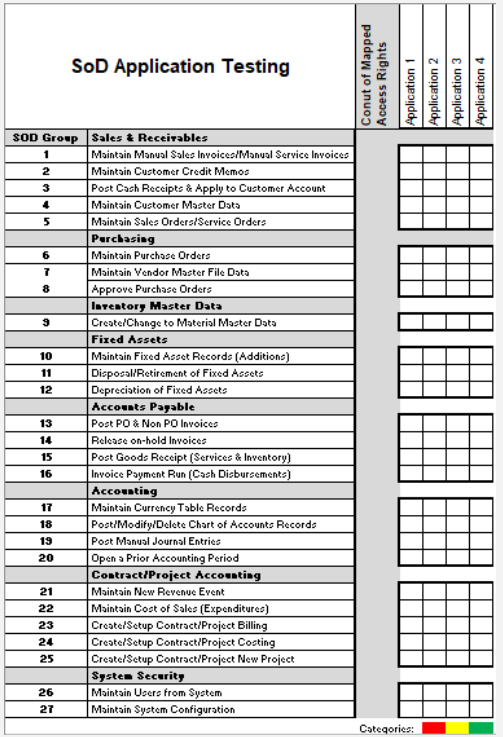
The importance of SoD is to ensure that complete control of a process or asset does not become the responsibility of a single individual. Through the process of assigning multiple responsible parties, HLI can reduce their exposure to organizational risks.

Separation of Duties (SoD) Application Testing

Before HLI business and IT systems owners modify or make changes to systems or applications, they will benefit by implementing the SoD application testing process.

This process provides the ability for to compare, prioritize, and manage changes that impact multiple owners and ensure that all parties impacted by changes are involved with the change process.

The SoD application testing process additionally ensures that there are multiple business owners and may be used in conjunction with the Mileage Chart.



SoD Application Testing		Count of Mapped Access Rights	Application 1	Application 2	Application 3	Application 4
SOD Group	Sales & Receivables					
1	Maintain Manual Sales Invoices/Manual Service Invoices					
2	Maintain Customer Credit Memos					
3	Post Cash Receipts & Apply to Customer Account					
4	Maintain Customer Master Data					
5	Maintain Sales Orders/Service Orders					
	Purchasing					
6	Maintain Purchase Orders					
7	Maintain Vendor Master File Data					
8	Approve Purchase Orders					
	Inventory Master Data					
9	Create/Change to Material Master Data					
	Fixed Assets					
10	Maintain Fixed Asset Records (Additions)					
11	Disposal/Retirement of Fixed Assets					
12	Depreciation of Fixed Assets					
	Accounts Payable					
13	Post PO & Non PO Invoices					
14	Release on-hold Invoices					
15	Post Goods Receipt (Services & Inventory)					
16	Invoice Payment Run (Cash Disbursements)					
	Accounting					
17	Maintain Currency Table Records					
18	Post/Modify/Delete Chart of Accounts Records					
19	Post Manual Journal Entries					
20	Open a Prior Accounting Period					
	Contract/Project Accounting					
21	Maintain New Revenue Event					
22	Maintain Cost of Sales (Expenditures)					
23	Create/Setup Contract/Project Billing					
24	Create/Setup Contract/Project Costing					
25	Create/Setup Contract/Project New Project					
	System Security					
26	Maintain Users from System					
27	Maintain System Configuration					
						Categories:

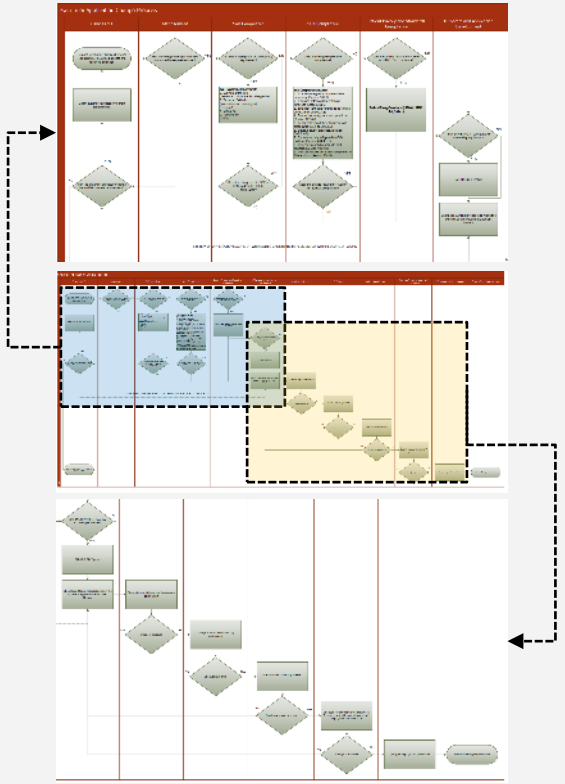
Change Management Process Diagram

Transitioning to a compliant SOX framework will require modifying the environment in which HLI is currently making changes to systems and applications. In order to reduce exposure to organizational risks and promote a fiscally sound auditing environment, HLI will promote a transparent process for authorization, approval, monitoring and testing changes.

HLI will also incorporate SoD for requesting/approving changes, moving programs into and out of production, as well as monitoring program development and changes.

This is also an opportunity to address process concerns within the development stages, including the implementation of subprocesses to promote application security and secure coding, as well as automating manual systems that are currently in place.

This process diagram highlights the new SOX and SoD process changes (blue/top) in conjunction with the current processes (yellow/bottom).

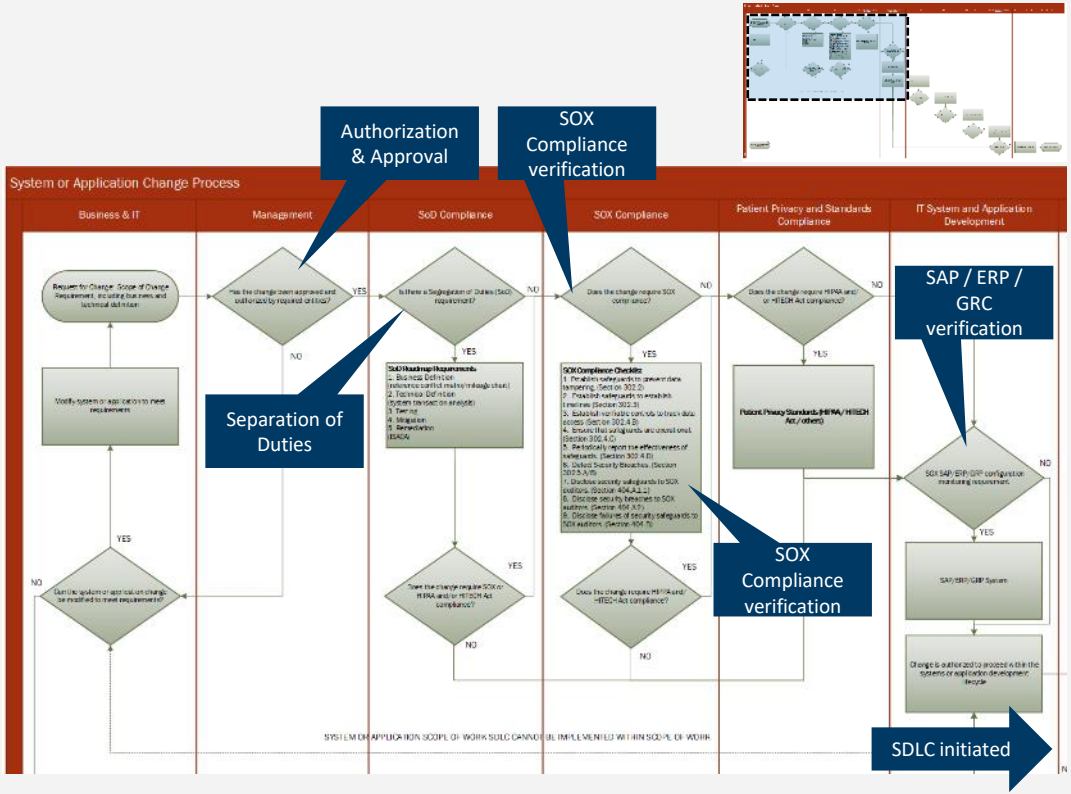


Change Management Process Diagram-SOX Compliance

This portion of the process diagram highlights the specific actions and requirements that HLI can implement to promote SOX and SoD requirements.

The system or application change is initiated, transitioned to management for authorization and approval pending compliance with SoD and SOX requirements, compares this change to requirement checklists as well as verification with the existing SAP system for auditing purposes.

Once the change has met these prescribed processes, it will transition to the systems or application development life cycle (SDLC).

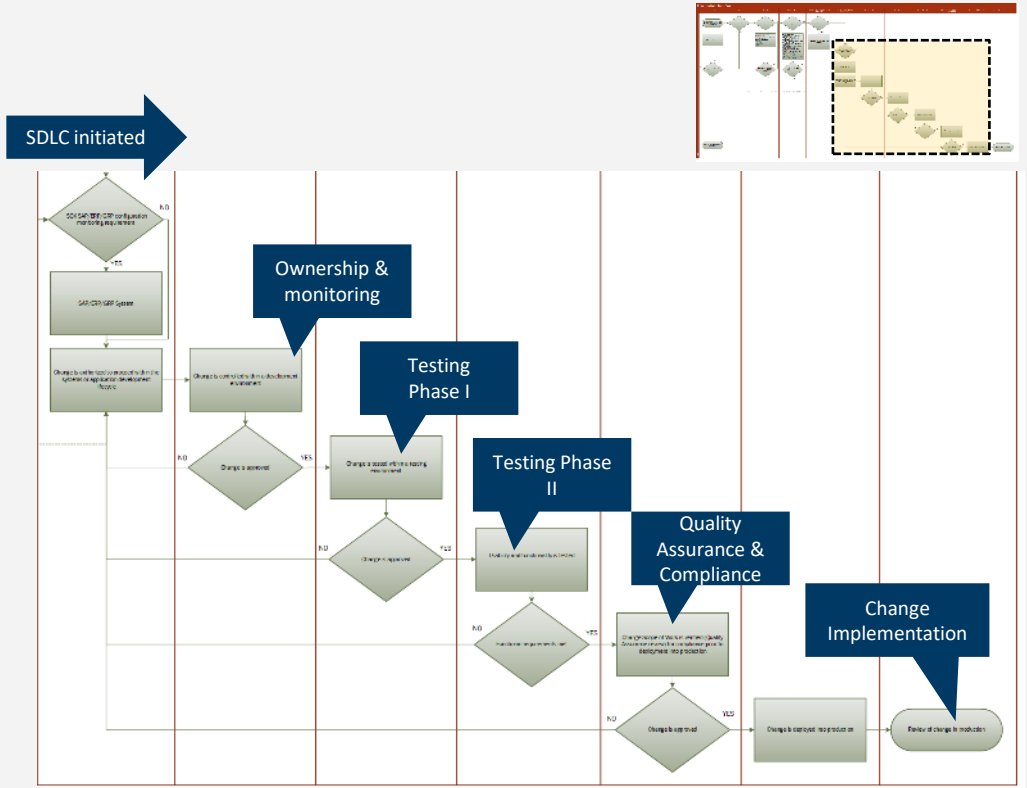


Change Management Process Diagram-SDLC Implementation

This portion of the process diagram continues from the previous, and includes the systems or applications life cycle (SDLC) initiation.

The change is led by a system or application owner and is monitored throughout the lifecycle of the change. The change is tested within a testing environment, followed by usability and functionality testing.

Once the change has passed these tests, the change will transition into quality assurance and compliance (verifying SoD and SOX), then implemented into production.

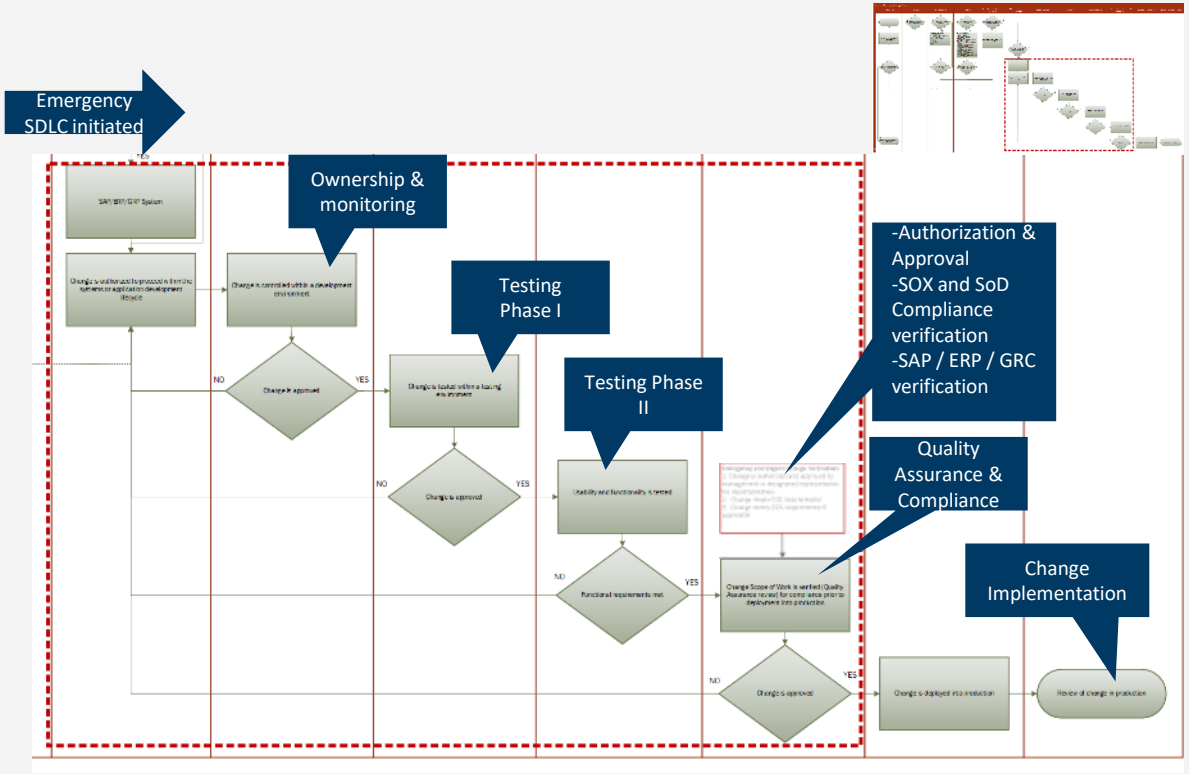


Change Management Process Diagram-Emergency Changes

This portion of the process diagram continues from the previous, and includes the systems or applications life cycle (SDLC) initiation.

The change is led by a system or application owner and is monitored throughout the lifecycle of the change. The change is tested within a testing environment, followed by usability and functionality testing.

Once the change has passed these tests, the change will transition into quality assurance and compliance (verifying SoD and SOX), then implemented into production.



Implementation and Compliance

Fortunately, SOX and SoD compliance will not be difficult for HLI to achieve.

With many of the current processes in place to manage and control changes within the SDLC environment, technical staff may not notice a big difference between current and future change management.

With additional process steps and proactive involvement with management and compliance, HLI is likely to embrace these changes and have a new framework which will promote their ability to transition from a private to a public company.

This new framework will also ensure that HLI is ready for quarterly and annually audits in compliance with SOX framework, as well as reducing their organizational risk exposure with separation of duties framework.

Section 2B: Logical Access Management (LAM)

What is Logical Access Management?

Logical Access, as opposed to Physical Access, is when you interact with hardware remotely to access information. According to technopedia.com, “This type of access generally features identification, authentication and authorization protocols.”

Logical Access Controls, are methods used to make sure only authorized users can access hardware remotely. Examples of controls include: “sophisticated password programs, advanced biometric security features, or any other setups that effectively identify and screen users at any administrative level.”

ISACA has identified authentication and access issues as High Risk.*

The impact of these risks can be of enduring severity, including (1) a mass customer data breach, (2) access by malicious actors, (3) attacks on the integrity or availability of data.

*IT Control Objectives SOX 3rd Edition, page 130.

HLI Specific Risks

After an initial risk assessment, HLI was found to have a comprehensive swathe of issues with Logical Access Management. Here is a short list of identified Logical Access Management issues:

1. Local representatives have access to comprehensive lists of members
2. All applications accessible to all employees
3. External website connects to internal Oracle database of all customers
4. Weak, user selected passwords and lax enforcement.
5. Credentialing issues
6. Admin access issues

The fundamental issues with HLI seem to break down into the following categories:

1. **Passwords**
2. Other Authentication issues
3. Privilege issues (as detailed by Saltzer and Schroeder)*
4. Design issues

*These issues breach many of the fundamental security principles outlined by Saltzer and Schroeder, including (1) separation of privilege, (2) least privilege, (3) Least common mechanism, and possibly (4) Complete mediation.

Focus: Passwords

As an example, we will outline a process to meet one of the LAM control objectives in Exhibit Two of the Case Document. Namely, passwords.

In the 2014 “IT Control Objectives for Sarbanes-Oxley” ISACA informs us that following the COBIT standards would satisfy SOX requirements for LAM. Despite references to DSS05.03 and other provisions of COBIT, a brief review of “COBIT5 Enabling processes” provides only the barest guidance on passwords.

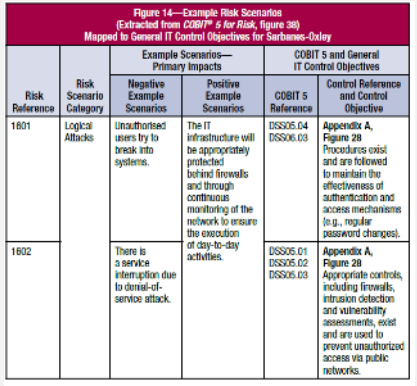
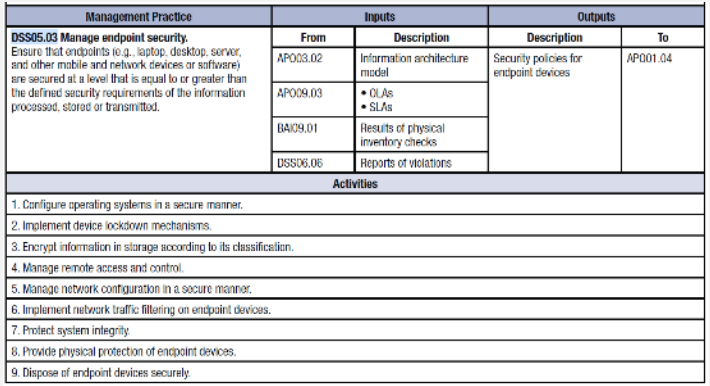


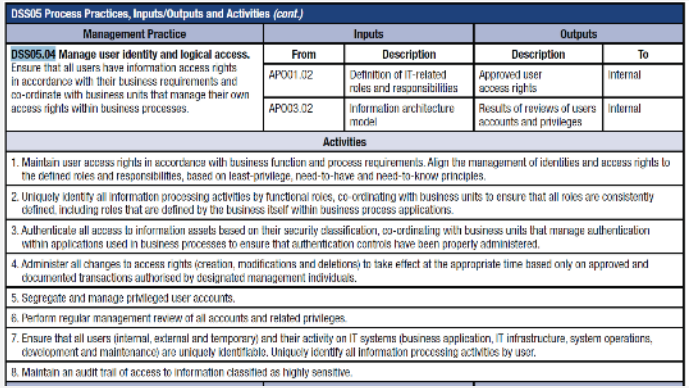
Figure 14—Example Risk Scenarios (Extracted from *COBIT® 5 for Risk*, figure 38) Mapped to General IT Control Objectives for Sarbanes-Oxley

		Example Scenarios—Primary Impacts		COBIT 5 and General IT Control Objectives	
Risk Reference	Risk Scenario Category	Negative Example Scenarios	Positive Example Scenarios	COBIT 5 Reference	Control Reference and Control Objective
1601	Logical Attacks	Unauthorised users try to break into systems.	The IT infrastructure will be appropriately protected behind firewalls and through continuous monitoring of the network to ensure the execution of day-to-day activities.	DSS05.04 DSS06.03	Appendix A, Figure 28 Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).
1602		There is a service interruption due to denial-of-service attack.		DSS05.01 DSS05.02 DSS05.03	Appendix A, Figure 28 Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access via public networks.



Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS05.03 Manage endpoint security. Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements of the information processed, stored or transmitted.	APO03.02	Information architecture model	Security policies for endpoint devices	APO01.04
	APO09.03	• OLAs • SLAs		
	BAI09.01	Results of physical inventory checks		
	DSS06.06	Reports of violations		

Activities
1. Configure operating systems in a secure manner.
2. Implement device lockdown mechanisms.
3. Encrypt information in storage according to its classification.
4. Manage remote access and control.
5. Manage network configuration in a secure manner.
6. Implement network traffic filtering on endpoint devices.
7. Protect system integrity.
8. Provide physical protection of endpoint devices.
9. Dispose of endpoint devices securely.



DSS05 Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes.	APO01.02	Definition of IT-related roles and responsibilities	Approved user access rights	Internal
	APO03.02	Information architecture model	Results of reviews of users accounts and privileges	Internal

Activities
1. Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.
2. Uniquely identify all information processing activities by functional roles, co-ordinating with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.
3. Authenticate all access to information assets based on their security classification, co-ordinating with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.
4. Administer all changes to access rights (creation, modifications and deletions) to take effect at the appropriate time based only on approved and documented transactions authorised by designated management individuals.
5. Segregate and manage privileged user accounts.
6. Perform regular management review of all accounts and related privileges.
7. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable. Uniquely identify all information processing activities by user.
8. Maintain an audit trail of access to information classified as highly sensitive.

Thankfully, various digested versions of the SOX/COBIT requirements exist.

Digests: Sources for Password Standards

IT Controls for SOX Audit (ITCSA), IT Controls Best Practices (ITCBP), and IT Control Objectives SOX 3rd Ed (ITCOSOX3) give COBIT level guidance on Authentication and access:

ITCSA:

1. One user id.
2. Use id based on personal information
3. Id should include numbers
4. Automatic locking after failed attempts
5. If not used in 90 days, id disabled.
6. Passwords at least 6 characters
7. Alpha & numeric
8. Upper and lower alpha cases
9. Password changes every 60 days
10. System history of 8 passwords

ITBP:

1. All user ids unique.
2. Auto log off after 30 minutes of inactivity
3. Lengthy, smart passwords
4. Never store passwords in plaintext
5. Password-aging features
6. Periodic forced password change
7. Mask passwords
8. Eliminate ids and passwords upon leave
9. Monitor activity
10. Least privilege

ITCOSOX3:

1. Procedures to maintain effectiveness of authentication and access.
2. Assess authentication mechanisms.
3. User time out.
4. No shared user profiles.

As you can see in the figure to the right, the password controls from the above ITCSA, ITBP, and ITCOSOX3 standards map almost identically to the ITGC password controls (figure to the right) required by HLI. Therefore, by implementing controls based on these standards, we can meet both the SOX requirements and HLI requirements without issue. The password issues include:

1. **Complexity**
2. **Expiration**
3. **Confidentiality**
4. **Exclusivity**

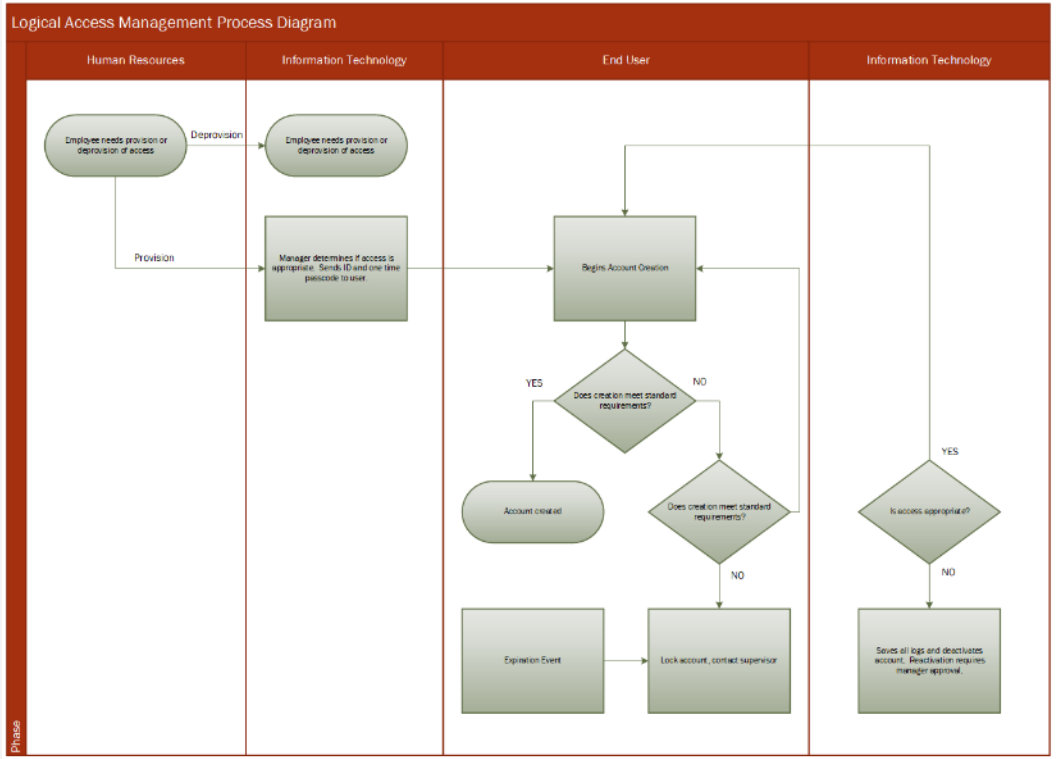
2	Password settings are appropriate	• For each relevant technical component of the logical access process, test the organization's settings for the following security configurations: ○ Minimum password length. ○ Initial log-on uses a one-time password. ○ Password composition (e.g., alpha/numeric characters, not words in dictionary). ○ Frequency of forced password changes. ○ The number of unsuccessful log on attempts allowed before lockout. ○ Ability of users to assign their own passwords. ○ Number of passwords that must be used prior to using a password again. ○ Idle session time out. ○ Logging of unsuccessful login attempts.

Proposed Login/Password Standards

1. Complexity
    - Passwords are alpha & numeric
    - Passwords have upper and lower case alpha.
    - Passwords minimum 8 characters.
    - No dictionary words.
2. Expiration
    - Auto-lock after 3 failed attempts
    - Auto-log off after 30 minute idle.
    - Credentials terminate if 90 day w/o use, or immediately upon departure.
    - Forced password change every 60 days.
    - Can’t use previous password.
3. Confidentiality
    - No plain text storage of passwords.
    - Masking of passwords.
4. Exclusivity
    - No shared user profiles.
5. Other
    - Monitor and logging activity
    - Periodic assessment of authentication system.
    - Self chosen passwords
    - Initial log on process, with auto generated one time password.

Process Owners, Steps, and Diagram

1. HR Representatives
    - Requests provision or deprovision of access upon employee hire/depart/report-of-issue.
2. IT Security Group (Supervisor & Manager: primarily focused on access)
    - Supervisor handles deprovision requests.
    - Manager handles initial provision request, sends permanent id and one-time passcode to End User if appropriate.
3. End User
    - Begins account creation by initial log on and setting of password according to guidelines.
    - Continues until account is created or failure occurs and account is locked.
    - In case of lock-out, termination of credentials, etc. contacts IT Security Group.
4. IT Security Group
    - Requests additional information from the end-user to authenticate, determines if access is appropriate then provides process to remake password or deactivates account.



Implement and Test

An initial overview of the HLI systems show that all actors and technology to implement the new heightened standards are in place. The board needs to merely set and mandate enforcement of the new access policies. The primary process owners and responsible parties are the supervisors and manager of the IT Security division.
For more help on testing the effectiveness of logical access controls: IT Controls Objectives SOX 3rd Ed (Figure 45 on 130) is beneficial. Though the proposed login standards should be sufficient to meet SOX standards.

Additionally, we recommend rolling out the new logical access mandates alongside:

Multi Factor Authentication; and

Although strong passwords increase Logical Access Security, it's far more effective if part of a comprehensive multi-factor authentication regime.
Adding tokens, phone-authentication, or geo-location would upgrade the authentication system to multi-factor.
Implementing Duo multifactor authentication is relatively cheap and straightforward, and will be covered again in the cost section.

Automation.

Much of the Logical Access Management process can be automated, saving time and reducing costs.

Design: Incident and Problem Handling

While the HLI IT support team may be amazing at their job, incident response is a formal process that requires a well-defined process and team. Members from IT support may be on the team, but the team should not consist solely of IT support.

To meet the requirements of SOX and HIPAA, as well as to maintain a secure environment, a formal and well defined incident response plan and team need to be in place.

HLI's obligations:

SOX section 302 and 404 require appropriate documentation for financial reporting. The appropriate handling of problems and incidents, along with reporting and audit trails, will meet this requirement. Additionally, with appropriate incident handling procedures, HIPAA requirements will also be met (especially, for example, subsection 164.308(a)(6)).

Design: Incident and Problem Handling

Establish a process that:

- Effectively and efficiently identifies and resolves incidents and problems
- Provides sufficient documentation and reporting for review and analysis

It is likely that some sort of software system (or systems) will need to be bought or built to provide reporting, log collection and analysis, ticketing, and tracking. A package like Zendesk (from $5 per month per user) may be useful for service requests and incidents for problem tracking, reporting, and ticketing.

To collect and analyze logs effectively, more advanced systems may be needed, and given the size of HLI may be less cost effective than building scripts in house for log collection and analysis.

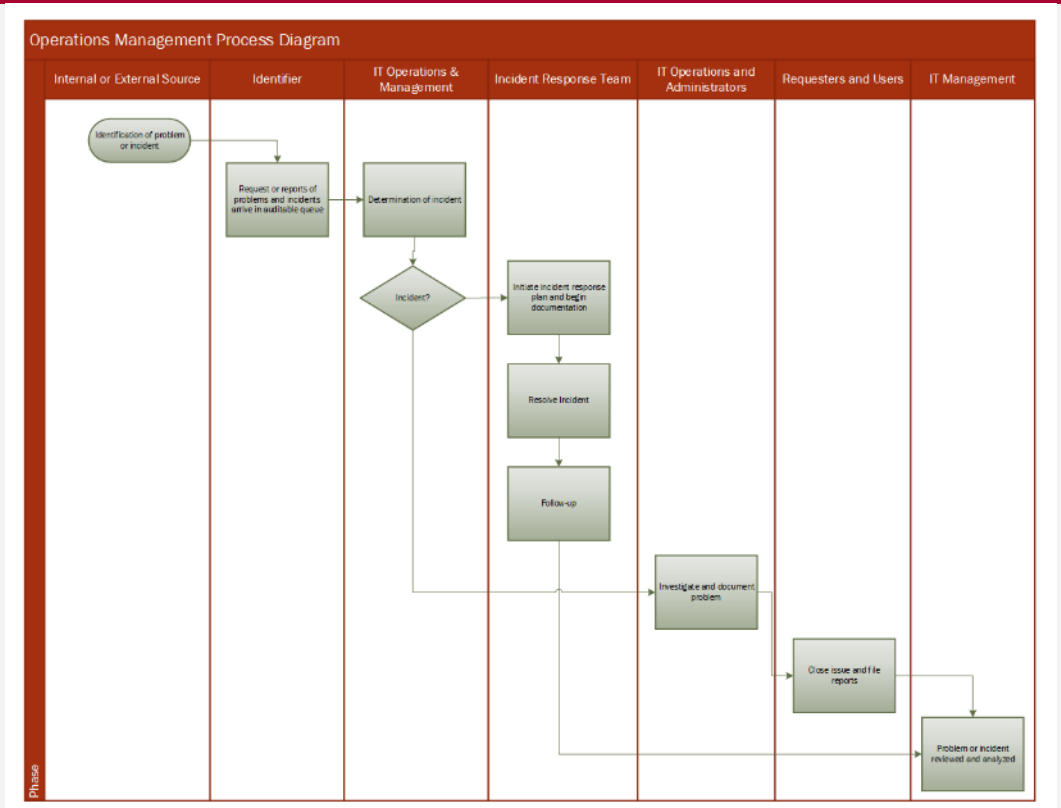
Building the incident response plan is an endless process, but may not necessarily require additional personnel. After an incident response playbook is built and a repeatable incident response process is established (framework for incident response in NIST 800-61r2, see Addendum 5 for a diagram of an incident response process), the team will be better prepared for an incident.

Design: Proposed process steps for incidents and problems

Process

1. Incident or problem is identified
2. Report is generated (sent to the tracking/ticketing system)
3. Determine if it is an incident?
    - Yes -> activate IRP (all steps of the IRP are documented)
        - Incident response team activates
        - Performs incident response process (e.g., contain, resolve, recover)
        - After incident has ended, after action reports are reviewed and determinations of what could have been done better are reported (follow-up)
    - No -> support manages problem and escalates as needed
        - Investigate and document problem
        - At resolution file reports and properly close issues
4. After resolution, documents of the problem or incident are reviewed and analyzed to determine steps to help prevent similar problems or incidents in the future

Operations Management Process Diagram



Implementation: Building the team and timeline

The incident response team is made up of roles that should already exist in the organization, so the costs for implementation will be limited to training and time spent. Roles should include:

- IT security experts
- Systems/network administrators
- IT technicians
- Disaster recovery expert
- Legal counsel
- HR

Timeline will depend on the establishment of formal process, but given the processes already in place, it is not likely to take more than a quarter to formalize the process if there is buy-in from the organization. There are templates available and there are step-by-step guides to building an incident response plan (e.g., https://www.exabeam.com/incident-response/incident-response-plan/ links to several resources for templates and step-by-step guides).

Implementation: testing

Tests include:

- Documentation that an incident management system exists and how it is used, and including management level documentation
- Review a sample of incident reports to determine if there was proper documentation, analysis, and resolution and that incidents were handled in a timely manner
- Determine if audit-trails exist for problems and incidents
- Review samples of the problem system to determine if it has audit trail and if it is being used
- Review samples of status reports and determine if patterns are being identified

Each of these tests provide for the ability to demonstrate that appropriate documentation exists such that it meets the requirements of maintaining integrity of financial data.

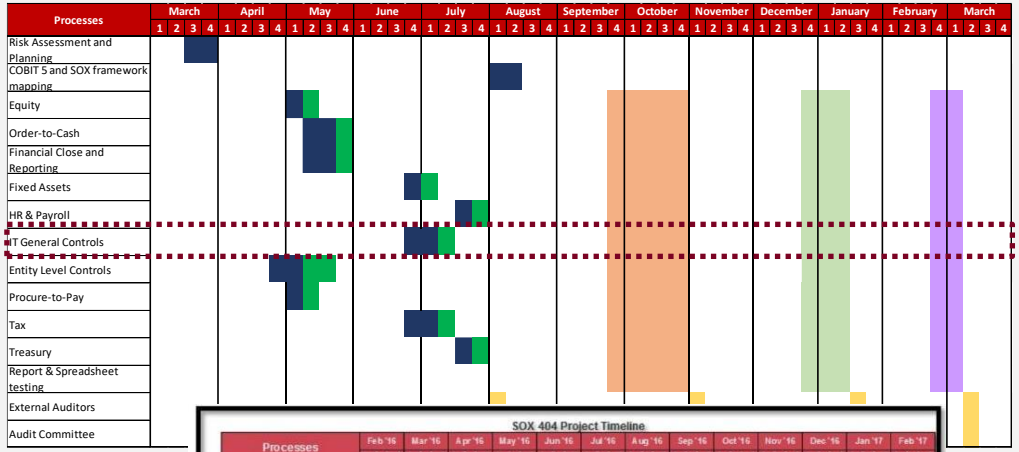
Section III: Timeline

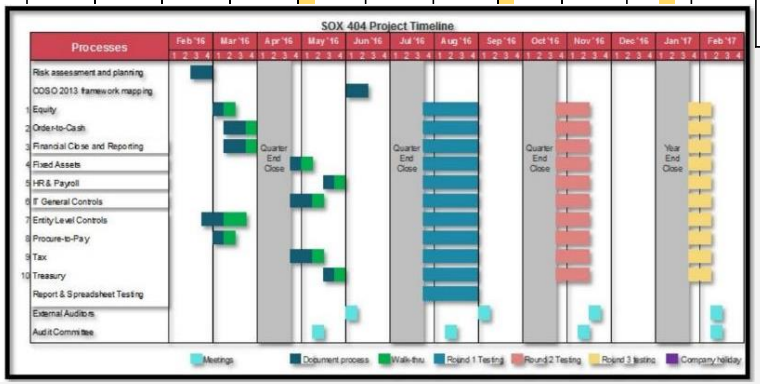
ITGC compliance is going to be part of a comprehensive change in the organizational framework to comply with SOX requirements.

The relevant IT related SOX sections 302 and 404 each have implementation times of approximately a year.

The initial IT control processes for CM, LAM, and OM are estimated to take 1-3 months to implement, though testing and finalization may take up to a year.

Additional recommendations may take additional time.





Timeline to SOX Compliance

Change Management (1-3 months depending on current configuration of SAP)

- Training
- Staffing
- Systems and Applications

Logical Access Management (1-3 months)

- Policy change (1 month): All people and systems are already in place, should take a limited time.
- MFA (3 months): Duo's 5 phased implementation framework will likely take at least 3 months *(see Addendum 3)*.
- Automation (1 month): Automation likely already exists in the system, and once policy is set, configuration merely needs to follow.

Operations Management (3 months)

- Primarily training time. Timeline will depend on the establishment of formal process, but given the processes already in place, it is not likely to take more than a quarter to formalize the process if there is buy-in from the organization.

Budget

Change Management:

Training for SOX compliance and patient privacy, basic for organization, advanced requirements for leadership and IT staff through. Learning management system, $5 per user per month. (estimated all staff for 1 month, IT staff for 3 months)

In support of organizational staffing objectives, HLI is seeking to hire three new personnel, including a Compliance Director, SOX Security Director, SAP consultant, as well as SOX compliance consultants (implementation process).

Logical Access Management:

Password Policy Changes: Free.

Multi Factor Authentication: Statefarm, a comparable company had 56,788 employees in 2018. The average price of Duo MFA is $3 a month, which comes out to $2,044,368 a year. (See Addendum 6).

Automation: Free (possible earnings from reduced man hours.)

Operations Management: See Addendum 4 for more details.

Budget

Component	Quantity	Cost	Multiplier	One-time Fee	Total Annual Cost-Year 1
Compliance Training-Learning Mgmt System	56,788	$5.00	1		$283,940.00
Compliance Training-Learning Mgmt System	150	$5.00	3		$2,250.00
Staffing-Compliance Manager	1	$200,000.00			$200,000.00
Staffing-Security Manager	1	$200,000.00			$200,000.00
Systems-SAP Consultant	1	$50,000.00			$50,000.00
SOX Compliance Consultants	4			$50,000.00	$200,000.00
Multifactor authentication training-basic	150	$50.00			$7,500.00
Multifactor authentication training-advanced	20	$500.00			$10,000.00
Duo Access Software application	56,788	$3.00	12		$170,364.00
Security training-basic	150	$300.00			$45,000.00
Security training-advanced	20	$7,000.00			$140,000.00
Security Software (lump sum)	1			$200,000.00	$200,000.00
External security consultant services	1			$100,000.00	$100,000.00
Audit (internal)	1			$25,000.00	$25,000.00
Audit (external)	1			$50,000.00	$50,000.00
					$1,684,054.00

Section 5: References

- O. Michael, "H.R.3763 - Sarbanes-Oxley Act of 2002", *Congress.gov*, 2002. [Online]. Available: https://www.congress.gov/bill/107th-congress/house-bill/3763/text.
- IT Governance, Risk and Controls Tool Kit: Process Documentation Form. J. Greis, J. Dennis. Information Technology Risk Management, Indiana University, Kelley School of Business, IT Tool Kit.
- "Subscriptions | Elastic Stack Products & Support | Elastic", *Elastic.co*, 2022. [Online]. Available: https://www.elastic.co/subscriptions.
- "Zendesk Pricing", *Zendesk*, 2022. [Online]. Available: https://www.zendesk.com/product/pricing/.
- "HITECH Breach Notification Interim Final Rule", U.S. Department of Health & Human Services, 2013. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html.
- "The HIPAA Privacy Rule", U.S. Department of Health & Human Services, 2021, [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
- Cassetto, Orion. "Incident Response Plan 101: The 6 Phases, Templates, and Examples", Exabeam, 2022, [Online]. Available: https://www.exabeam.com/incident-response/incident-response-plan/.
- "How Much Does an LMS Cost? 2022 Pricing Guide", Better Buys, 2022. [Online]. Available: https://www.betterbuys.com/lms/lms-pricing-guide/.
- Information Systems Audit and Control Association (ISACA), *COBIT 5*. Rolling Meadows, IL: Information Systems Audit and Control Association (ISACA), 2013. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0.
- Information Systems Audit and Control Association, Internal Control using *COBIT 5*. Rolling Meadows, IL: Information Systems Audit and Control Association (ISACA), 2016. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004LF0QEAW.

Addendum

Addendum 1: SOX Section 302

Who is responsible:

Enterprise's management, principal executive and financial officers

What they are responsible for:

Certifying officers-establish and maintain internal control over financial reporting

Providing reasonable assurance regarding the reliability of financial reporting and preparation of financial statements for external purposes in accordance with GAAP

Changes that have occurred during the most recent fiscal quarter which have the ability to materially affect the company's internal control

Reasons for changes and circumstances surrounding the change.

How Often:

Quarterly and annual assessments

Addendum 2: SOX Section 404

Who is responsible:

Enterprise’s management, principal executive and financial officers

What they are responsible for:

Certifying officers-establish and maintain internal control over financial reporting

Providing reasonable assurance regarding the reliability of financial reporting and preparation of financial statements for external purposes in accordance with GAAP

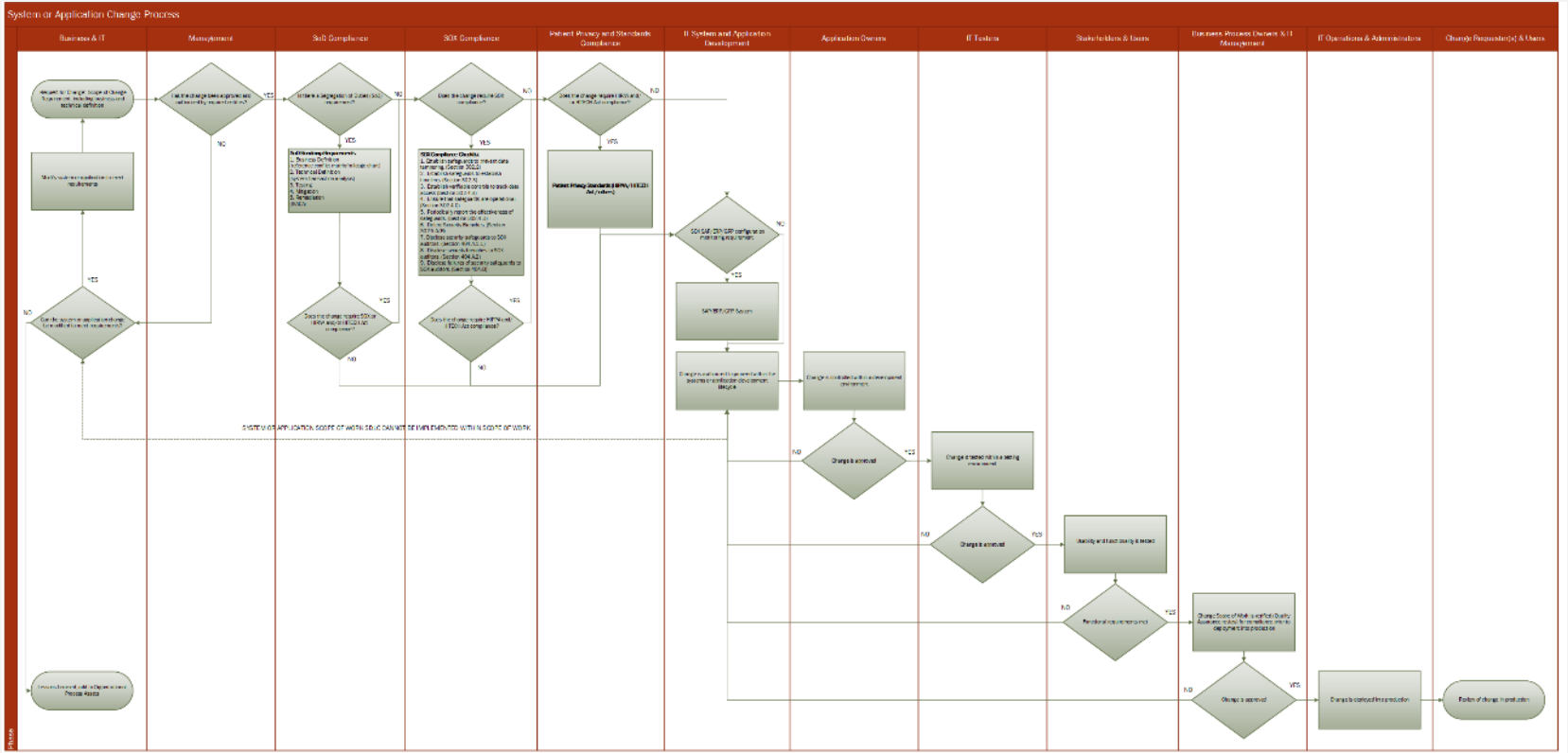
Changes that have occurred during the most recent fiscal quarter which have the ability to materially affect the company's internal control

Reasons for changes and circumstances surrounding the change.

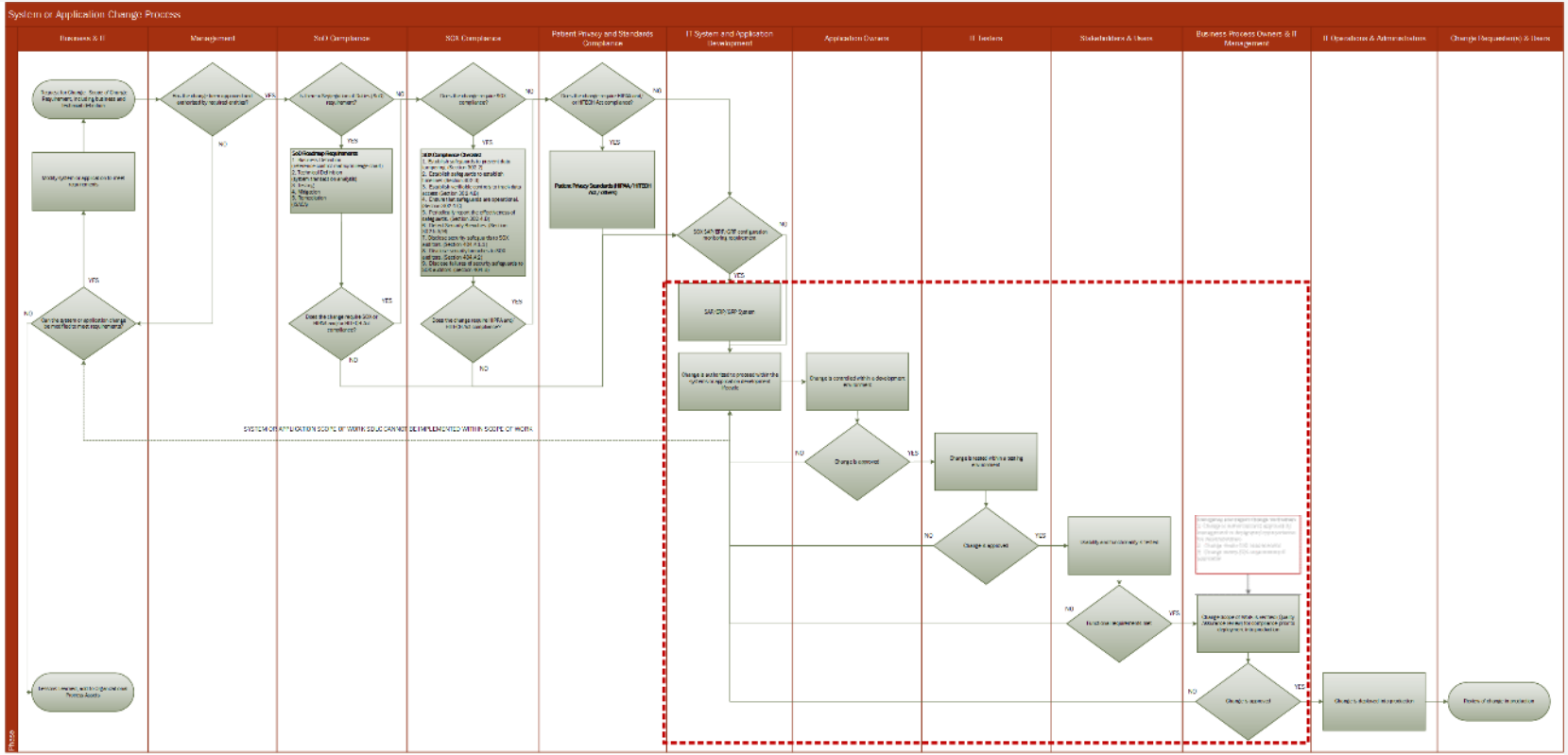
How Often:

Quarterly and annual assessments

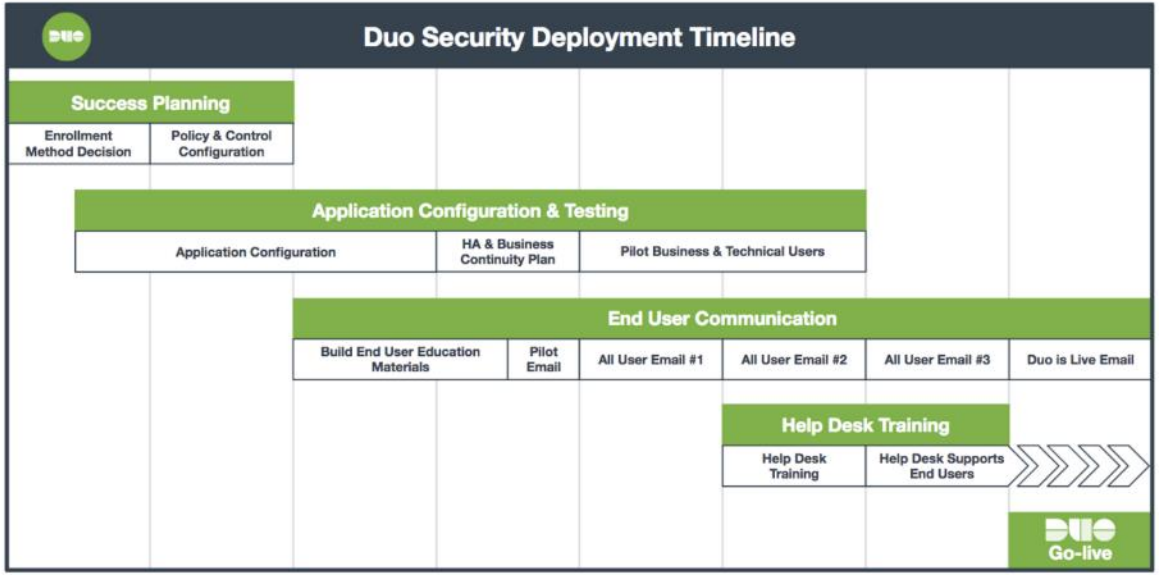
Addendum 3: Change Management Process Diagram



Addendum 4: Emergency CM Process Diagram



Addendum 5: Duo Security Deployment Timeline and Pricing



References:

https://duo.com/docs/getting-started

https://en.wikipedia.org/wiki/State_Farm (# of employees: 56,788)

https://duo.com/pricing (pricing for Duo services: 3 dollars per month)

Addendum 6: Operations Budget-details

Costs include:

- Staff (assume this already exists)
  - Salaries covered while training, conducting exercises, and otherwise engaged in incident response preparation or handling
  - Training could cost tens of thousands (SANS institute training costs around $7,000 per self study course: https://www.sans.org/selfstudy/)
- Software (assume most of the required software already exists
  - May need to invest in some log collection and analysis software upgrades or replacement of service desk software
    - ELK cloud starting at $16/month for basic services (https://www.elastic.co/elasticsearch/service/pricing)
    - Zendesk starts at $5 per month per user (https://www.zendesk.com/product/pricing/)
- External services (retaining legal and forensic services)
  - Likely to cost >$100,000 in the event of an incident (e.g., forensic services could cost up to $100,000 in some instances [https://www.vestigeltd.com/thought-leadership/digital-forensic-services-cost-guide-vestige-digital-investigations])