

# Compliance

## Sarbanes-Oxley

## FastPass Password Manager and Sarbanes-Oxley Compliance Requirements

**A well-run, self-service and automated password management process will help IT Managers and Governance Risk Managers face some of the difficult challenges of Sarbanes Oxley Section 404 compliance. Requirements that in many area are similar to those from other governance institutions like HIPAA, ISO and European Union.\***

This document discusses how IT managers can use a password management tool as a first bite approach to deploying an identity and access stack in order to respond positively to Sarbanes-Oxley (SOX) requirements.

The big change to the way organizations respond to SOX comes in the handling of internal controls. In practical terms this means SOX requires process examinations that reach to the lowest levels of the Corporation.

To meet a SOX audit, companies have to show that the way they measure and conduct themselves is correct, open to authorized examination, and not subject to corruption or manipulation. In addition, SOX requires corporations to report problems that substantially affect financial reporting immediately. IT specific scrutiny comes from three provisions of the act: Sections 302, 404 and 409.

- Section 302 requires corporate executives to certify that adequate controls are designed and implemented to assure financial reports are reliable and compiled according to "Generally Accepted Accounting Principles" (GAAP).
- Section 404 requires that the Section 302-controlled processes result in certifiable financial reports. These sections mean that management must exercise continual scrutiny of the integrity of the financial reporting process, including the underpinning technology. Consequently, IT managers must take responsibility for the integrity of the IT role in the financial reporting process.
- Section 409 states that material changes require immediate public disclosure, placing further reporting burdens upon the IT organization.

### SOX Compliance and IT

IT management must be aware of financial functions on a very granular level and have procedures in place to deal with the business implications of IT activities. The issue for IT is to introduce awareness of business functions to the technical disciplines that are the foundation of IT.

To accomplish this, IT managers have to understand and implement the same procedures practiced in governance of non-IT areas of business. Identity and Access processes are critically important to the "well-being" of the organization and automation driven software applicable to the problem must be deployed.

CobiT (Control Objectives for Information and related Technology) is the widely accepted source amongst auditors for defining control objectives in IT governance and was released by two respected auditing professional associations, the Information Systems Audit and Control Foundation and IT Governance Institute. It represents wide consensus among IT auditors because CobiT systematically analyses IT defines general control objectives, performance indicators, and maturity models for IT.

\* see page 4

### Benefits of having an automated password management in place

- Full, automatic audit trail
- Time stamped open and close dates
- Easy classification of actions and incidents
- Document's the scope and consequences of any violation
- Easy access to knowledge documentation

Password security  
made EASY

The CobiT control objectives go beyond financial reporting and extend to all functions of IT. However SOX auditors are only concerned with financial reporting. At audit time, SOX auditors use prepared questions and checklists to assess the quality of internal controls on financial reporting. Each auditing firm has their own method based on their choice of frameworks, and CobiT is frequently the source of their methods. Therefore, an IT department seeking SOX compliance can be reliably guided by CobiT, not only in financial reporting, but in all areas of IT governance.

In practical terms, each control objective corresponds directly with a control activity. A control activity is something done to attain a control objective. For example, "IT security administration monitors and logs security activity and violations are reported to senior management" is an illustrative control objective from the IT Governance Institute. A corresponding control activity is to "establish a data security system". Control activities can be pro-active (preventative) or reactive (detective). Establishing a security system is pro-active, but finding security breaches after they have occurred is reactive. Both pro-active and reactive activities are necessary to attain control objectives, but pro-active activities are clearly more powerful. Control activities are also classified as automatic and manual. An automatic control activity does not require human intervention and is usually more desirable than manual activities.

### The Password Management Application

In addition to being a control objective in itself, an IT department will find that automated self-service password management will execute many of the control activities necessary for adequate IT control over financial reporting and other areas of compliance. For departments that already have adequate controls, a password management application can automate manual processes and convert manual control activities to automatic activities. Manual control activities depend too much upon the mood of the people who execute them. An automatic activity does not have good days and bad days and its attention never wanders.

The application has two main functions:

1. The first function empowers Information Workers to be able to enroll themselves and reset their passwords using a web based self-service interface to a challenge and response engine residing on the domain controller.
2. The second function records and manages access attempts, enrollments, password resets whether successful or failed, date and time and user profile and location by IP address. The software can enter a ticket automatically to a Helpdesk application and simultaneously close or notify according to the help desk configuration. Notification by means of automated logging removes any human element of failure.

### FastPass Password Manager and Control Objectives

FastPass tools are in themselves a control objective. The IT Governance Institute suggests for SOX compliance, "Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution".

The institute goes on to explain

*"Managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. Deficiencies in this area could significantly impact financial reporting".*

Good password management practice is therefore a requirement for good IT governance and SOX compliance. However, the usefulness of good password management practices and software goes far beyond this because the software aids in meeting other required control objectives.

## FastPass Features for SOX Governance

A basic password management implementation provides manual detective control activities as well as proactive and automated control going beyond manual, detective activities and making the implementation of automatic preventive activities straightforward and effective. At the most basic level, for detective control activities, the application records incidents clearly. Whether the application is acting in a detective or preventative capacity, clear recording of the essential information is important because the system records the data automatically. The system must record the action, the date and time the action occurred as well as the responsible user profile. An unambiguous audit trail must be recorded as events evolve to provide evidence that all this happened. FastPass Password Manager provides this functionality.

This feature list is what makes FastPass Password Manager a useful application for the enforcement of SOX compliance requirements:

- **A full, automatic audit trail** to track all changes activities associated with enrollment and password reset.
- **Time stamped open and close dates.** Tampering with these dates is impossible. Timestamps are inviolable.
- **Easy classification of actions and incidents** by the action, location, user profile, date and time of subject matter.
- Tickets can be generated **documenting the scope and consequences of any violation.**
- **Easy access to knowledge documentation** on the associated control objectives and activities.

For preventive activities, the application should support ITIL incident and problem management processes. This practice of identifying the problems that cause incidents and rectifying them to forestall future incidents is resolved with FastPass Password Manager by "outbound integration" to Helpdesk applications for automatically recording user access and authentication activities. In conjunction with other tools in the FastPass stable, FastPass Password Manager has many exit points for automatically launching additional password management control activities to other systems when initiated from an Active Directory self-service password reset.

The result is that FastPass Password Manager acts as the focal point of several automated control activities. Using FastPass Password Manager outbound integration to Password Account Manager or Microsoft Identity Lifecycle Manager (ILM 2/2007) could enable account claims on other vendor systems for Identity mapping to facilitate future password propagation or alternatively verify accounts on target systems for ILM2/2007 Management Agents to affect future password propagation.

*FastPassCorp A/S is a global provider of self service solutions for password management and beyond. FastPassCorp A/S is a leading provider of self-service password management solutions ranked in the global Identity & Access Management category. FastPassCorp A/S is listed on First North, OMX Copenhagen Stock Exchange (FASTPC) and is headquartered in Greater Copenhagen area, Denmark.*

Self-service automated password propagation across the organizations environment is further supported by an add-on *password filter* to the Active Directory for integrating password policies in disparate systems and standardized logging supports the possibility of standardized reports for all access attempts on all systems for all users. This is an opportunity to implement controlled procedures as control activities throughout the environment. In conjunction with basic workflow functionality, requests for access to systems can be granted according to the role of the user making the request and that the correct level of access is assigned to complete the request. Once again, "outbound integration" can provide automatically traceable and auditable records of the request for access. Follow up cross-referencing of system logs with the request log provide a robust detective control on access to the system while enforcing the automated procedure.

**FastPass Password Manager's ability to deliver both detective and preventive control activities through self-service and automation will help meet many different SOX and other compliance challenges.**

An IT department uses FastPass to lower operational cost, increase the password reset security model and to promote user productivity whilst automatically monitors the unexpected events that stop or threaten delivery of services.

Not all SOX control objectives deal with unexpected events, but with an environment configured to respond with the appropriate control activity, the IT department will achieve two things:

1. The incident receives the proper response with an auditable record.
2. An automated procedure is in place to show the auditors that the IT department will always respond to these incidents consistently and properly. And in addition securely taking care of the potential human error risk.

---

**\* Examples of other regulative bodies that requires attention and action:**

**HIPAA Security Rule:**

*"164.312 (a)(1) Assign a unique name and/or Number for identifying and tracking user identity."*

*"164.312 (d) Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*

**PCI DSS – Regulation 8:**

*"8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows..."*

**European Union Directive 95/46/EC:**

*"Article 17 ....must implement appropriate technical and organizational measures to protect personnel data against ...unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network..."*