IT Compliance
Best Practices Report

Overview

As an IT leader within your organization, you face new challenges every day – from managing user requirements and operational needs to the burden of IT Compliance. Developing a strong IT general controls environment helps your IT shop deliver services with quality, but there is overhead associated with these controls. What if you could enhance the quality of your control processes and reduce the amount of overhead on your staff at the same time?

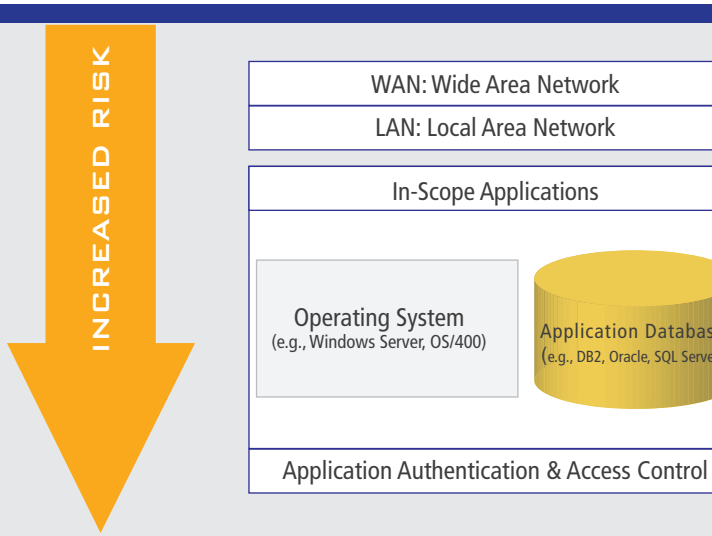
This IT Compliance Best Practices guide was designed to help you identify opportunities to streamline your compliance processes and implement automation. We've leveraged our experience helping organizations implement efficient and effective control environments to develop guidance that we hope you will find useful. This guide is organized around the three primary aspects of IT general controls:

- **MANAGE CHANGES TO SYSTEMS**
- **RESTRICT LOGICAL ACCESS TO SENSITIVE DATA & APPLICATIONS**
- **MANAGE DATA & OPERATIONS**

Considering Risk

An important concept in streamlining your IT compliance approach is to evaluate the risk within your IT infrastructure as it relates to in-scope applications and services. In our experience, we've found that as control procedures move closer to the underlying inscope applications (e.g., managing user access within your ERP system) they become higher risk and more important to your auditors. Conversely, control procedures that are further away from your core applications (e.g., monitoring security events on your firewall) tend to have lower risk to your financial reporting processes and are of less interest to auditors.

We encourage our clients to focus their efforts on areas that directly impact the highest risk areas. In many cases, your control procedures can be streamlined to enhance your overall IT general controls environment while actually reducing the amount of effort expended.



Consider alternative procedures for low risk areas. For instance, document your review of weekly antivirus reports instead of the daily threat alerts. Perform a quarterly or semiannual review of open ports on your firewall instead of daily log review.

Put more emphasis on access control that is within your ERP and other in-scope applications, and the change management process followed for their maintenance.

Managing Changes to Financial Systems

Automated business systems are the focal point of most IT general controls environments. These systems are the primary driver of the financial reporting process and their maintenance must follow a set of key controls to ensure errors are not introduced. To ensure IT compliance, you need an audit trail of key control points within your Software Development Process ("SDP") as well as ongoing monitoring of activities.

Best Practices

Standardize your software development processes —

If you have multiple applications that require IT compliance, significant gains in efficiency can be obtained by standardizing your development processes. Even if these applications are managed by different groups or run on different platforms, following a standard SDP reduces the amount of documentation maintained, simplifies training and operations, and will allow your internal and external auditors to consolidate their evaluation and testing efforts.

Evaluate changes based on risk —

Not all changes to your applications are created equal. In many environments, the number of changes with potential impact on financial statements is relatively small compared to the overall number of changes. In these situations, evaluating and categorizing changes as minor versus major may allow you to use a streamlined approach. Dedicating the bulk of your efforts towards high risk projects improves quality and reduces the risk of a compliance failure.

Use monitoring controls —

In many environments, it's difficult to guarantee a complete separation of programming and operations duties because of staff size or limited knowledge of a specialized technical environment. Implementing detect controls, such as monitoring changes that occur in a production environment, can often compensate for this lack of segregation. They are also very helpful as non-key controls that can provide the necessary assurance in the event one of your key preventative controls fails.

Maintain separate logical IT environments using VM templates —

Separate environments should ideally be maintained for development, QA, staging, and production. One effective way to maintain these environments is to use virtual machines that can be deployed as necessary without the need for additional hardware. By starting with a base template that includes the core environment, these logical servers can be quickly deployed and retired as necessary without need for additional hardware and minimal product installation time.

Provide key performance indicator updates to management —

Key Performance Indicators (KPIs) should be captured as a routine part of the change management process, and should be evaluated by management to alter or adjust procedures and practices. Although this is typically not part of your IT general controls procedures, it provides a strong entity level control. KPIs should include number of changes by system, number of bugs versus enhancement, number of patches versus upgrades, and other indicators that provide insight into the volume and quality of changes.

Automating Your Change Management Process Can Simplify It Compliance While Yielding Significant Improvements In Quality.

Questions to ask yourself

If you can't answer "yes" to all of these questions, you probably have an opportunity for improving your compliance processes.

- ☑ Have we eliminated the need for manual documents to track key control points within our SDP?
- ☑ Can we generate a list of changes by system affected?
- ☑ Can we provide assurance that the changes placed in production are the same as those which were approved?
- ☑ Can we quickly identify the modules affected by each software change?
- ☑ Can we obtain sign-offs for each step of the SDP electronically?
- ☑ Does our SDP include infrastructure changes and other types of maintenance?

Most methodologies follow an authorize, design, code, test, approve, and deliver process similar to the one shown above.

Managing Logical Access to Key Systems

Access to financial systems and data must be properly secured to ensure IT compliance,but it's always been an IT best practice to ensure proper security is in place. Let's face it … users can't break things they don't get their hands on. Managing user access typically follows detailed procedures that require approval for provisioning and removing accounts. Augmenting these procedures with proper detect controls can enhance your control environment as well as provide a safety net for the times that something goes wrong.

Best Practices

Standardize user provisioning and termination processes —

Most companies have a variety of systems that require user accounts (Windows Active Directory, VPN, ERP system, etc.). Although the types of access available might vary, the general process for obtaining and removing access can usually be standardized. The key control points for obtaining approval, documenting the access required, and recording the final resolution of the request are basically the same. Standardization will simplify your processes and support a consolidated evaluation and testing approach.

Consolidate and automate monitoring processes —

Security events occur within each layer of your infrastructure. These events begin with your firewall and perimeter network, continue through your local area network, and end with your ERP system and database. A single log monitoring solution can be used to monitor all of these events and reduce required maintenance.

Consolidate compliance functions within a single help desk system —

Most key control procedures related to system security, such as event monitoring and user provisioning, can be managed with a single help desk system. This allows you to directly associate the events generated from your monitoring controls with your prevent controls. For instance, you can associate the ticket generated from a completed user termination request directly with the windows active directory event (ID 630 in Windows 2003) that is triggered when the account is deleted. This becomes very useful when there is delay closing the termination help desk ticket or manual sign-off forms contain an incorrect date or clerical error.

Manage access to administration passwords —

Administration passwords are the keys to your IT castle and protecting them is typically one of the controls within the logical access environment. On the other hand, your IT staff must have ready access to this information to perform their duties as administrators. The traditional method of storing admin passwords in a physical location, such as a safe or locked cabinet, is difficult to maintain and provides weak authentication protection. A better method is to store this information in a secure location electronically where access control can be easily managed and monitored.

Automating your logical access control processes can simplify your IT Compliance process, but also yields significant improvements in quality.

Questions to ask yourself

If you can't answer "yes" to all of these questions, you probably have an opportunity for improving your compliance processes.

- ☑ Have we replaced manual reviews of event logs with automated event monitoring?
- ☑ Have we documented all of the events that are classified as "significant" and defined the required actions?
- ☑ Do we have pre-written templates for each event follow up action to ensure actions are properly documented?
- ☑ Can we provide evidence that appropriate action was taken for each significant event?
- ☑ Do we send notifications to appropriate staff whenever an event occurs that requires their attention?
- ☑ Can we search our history of events and generate reports for each type of event?
- ☑ Do we have an escalation process that monitors the status of unattended events and notifies management when events are not resolved timely and at risk of deficiency?
- ☑ Do we have an automated user request process that captures all required request information?
- ☑ Can we generate custom forms as needed to capture user request information without hand coding and maintaining HTML?
- ☑ Do we store admin passwords in an electronic format and control access electronically?

Managing Your Operations Process

Operational processes, such as performing backups and managing job schedules, are critical to the ongoing accuracy of your financial reporting systems. Key controls in this area typically focus on ensuring the underlying data used within these systems are safe and up to date and that systems are properly configured.

Best Practices

Use backup notification processes —

Most backup applications provide the ability to generate notifications upon completion, including a complete copy of the backup log. Similarly, job schedulers have the ability to generate status messages that can provide evidence of job completion. Whenever possible, it's best to automate these types of status messages rather than relying on a manual review of screens, reports or other processes that require manual intervention.

Focus on high risk scheduled jobs —

The number of scheduled jobs that pose a significant risk to financial reporting or operations is typically small. For many of these jobs, there are compensating manual controls or procedures that would quickly identify issues with the job. Focus your efforts on the remaining high risk jobs by documenting the nature of scheduled jobs and automating a notification upon completion of your scheduled jobs. You can then develop a filter to review these notifications and identify job failures that require action.

Your backup and job scheduling activities are prime targets for automation. Consider the following options.

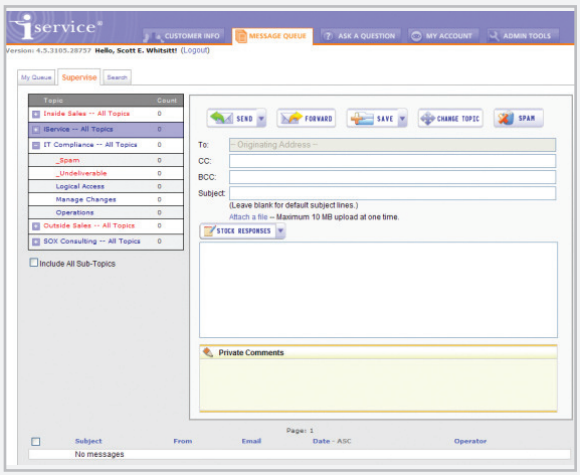
Questions to ask yourself

If you can't answer "yes" to all of these questions, you probably have an opportunity for improving your compliance processes.

- ☑ Does our backup job process include a notification with attached log files?
- ☑ Are our notifications going to a central repository with auto generated tickets rather than an individual's email account?
- ☑ Do we have pre-written templates for follow up actions on backup jobs to ensure actions are properly documented?
- ☑ Can we provide evidence that appropriate action was taken for any failed backup or scheduled job?

The iService Advantage

Now that you've thought about streamlining your IT shop's compliance efforts, imagine the benefits of a system that has all of these activities pre-defined for you! Working with the leading email response management and workflow product, iService, we've done exactly that. You can now implement a solution that will help you automate many of your routine processes, and use a template that has the following features out of the box:



- *Filters that automatically categorize important security events, along with stock answers for most events.*
- *Automatic form generation for user requests with the most common fields predefined.*
- *Service level monitoring and reporting for management to ensure your organization stays compliant.*

iService

A summary of the more common compliance challenges and the solutions provided by iService are shown below.

COMPLIANCE ISSUE	SOLUTION	BENEFITS
Important security events are generated within various systems, and manual review is time consuming and typically ineffective. Documenting these types of reviews is prone to error and provides weak evidence.	In conjunction with event monitoring and notification, iService provides preconfigured filters that evaluate and categorize each notification. Significant notifications can trigger alerts to staff as needed. Events are stored in a secure database indefinitely.	Eliminates manually review of event logs, and creates an audit trail for each significant event in a single and easy to use system. The ability to search events by type reduces compliance audit effort.
Follow up actions on events are often inconsistent and not documented.	iService includes suggested responses for each event type that can be selected from a handy drop down menu.	Pre-written responses provide guidance to staff, ensure consistent documentation, and save time.
Multiple events can be generated in certain scenarios, and documenting the actions taken can be overwhelming.	Using the mass update feature, multiple events can be handled with a single response.	Ability to mass respond to notifications saves time when dealing with multiple event notifications that required the same or no follow up action.
Manual review of event logs can't be monitored, and if event notifications are sent to staff email accounts there are no escalation options.	iService includes predefined alerts to notify management when notifications have not been closed timely, or user requests are approaching their service level.	Management will always be informed before security events go unnoticed, responses to user terminations exceed company policy, or other issues become deficiencies.
Gathering documentation for auditors is time consuming and often requested multiple times.	Predefined SOX 404 compliance reports provide a complete summary for internal and external auditors.	Auditors get a complete view of activities and substantial staff time is saved.
Paper forms used to capture user requests are difficult to manage, and generating web forms to capture end user requests is time consuming and difficult for many IT shops to manage.	iService includes automatic form generation on a topic by topic basis that can capture as much custom information as desired.	Requests are more complete and new forms can be generated in minutes. The data captured is available to other processes within the enterprise and can be used in various metrics and reports.
It is difficult for management to gain insights into the IT Compliance process, and often only discovers issues when they are reported as deficiencies.	The iService IT Compliance dashboard provides real-time insight into various activities that affect compliance and IT Governance.	Management is aware of key activities and has the ability to measure performance across a broad range of key areas.

These are just a few of the features and benefits that you can derive from a properly configured iService compliance system. And since iService is an enterprise level CRM solution with applications beyond IT Compliance, your investment can be leveraged across the enterprise into areas like your contact center, help desk, human resources, and any other aspect of business that manages a large number of interactions.

To learn more about the IT Compliance version of iService or services provided by IT Compliance Experts, contact Scott Whitsitt at 217-903-4458 or Scott.Whitsitt@ITComplianceExperts.com.