

SOLUTION BRIEF

Maintaining Sarbanes-Oxley Compliance: How Tripwire Helps



"We know it will only be a matter of time before we need proof of our change control policy and process. So, we are trying to stay ahead of the curve and provide auditors with the detail behind our process."

— Ian Wolff
Security Engineer,
Pulte Mortgage



Sarbanes-Oxley (SOX) requirements resulted in IT organizations scrambling to implement internal controls over their financial reporting, operations, and assets. Since the initial deadlines have passed, public companies that are subject to SOX governance have achieved at least a basic level of control over financial systems—and by extension—their underlying IT operations. So what is next?

The answer is *sustaining* compliance. In the limited amount of time that was available for organizations to become compliant, it was difficult for many to determine the ongoing impact of the new controls on costs, processes, or operations. Now, IT organizations must fine-tune their controls and processes so that they can meet another important SOX requirement: regularly disclosing information about the viability of these controls and potential fraud or losses that may affect the company's financial position.

To successfully sustain compliance, organizations must implement best practices to ensure IT systems not only achieve a known and trusted state but they also

maintain that state. Achieving a known and trusted state is a challenging task for even the most technically adept organizations but this approach results in reduced security risk, increased system availability, and lower audit costs. Many organizations rely upon Tripwire configuration audit and control solutions as an integral element of their sustained compliance initiatives. Tripwire enables companies to automate the continuous testing and reporting of critical IT process controls to provide a detailed audit trail in support of SOX requirements.

Taking a Long-term View

A sustainable compliance posture must address the control, evaluation, and disclosure elements of SOX Sections 302, 404, and 409. To do so, many organizations are beginning to adopt a standard framework, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The U.S. Securities and Exchange Commission (SEC) recognizes COSO as the official framework for establishing internal controls over financial reporting. The IT-specific aspect of the COSO framework is known as Control Objectives for Information and related Technology, or COBIT.

Meeting the Requirements

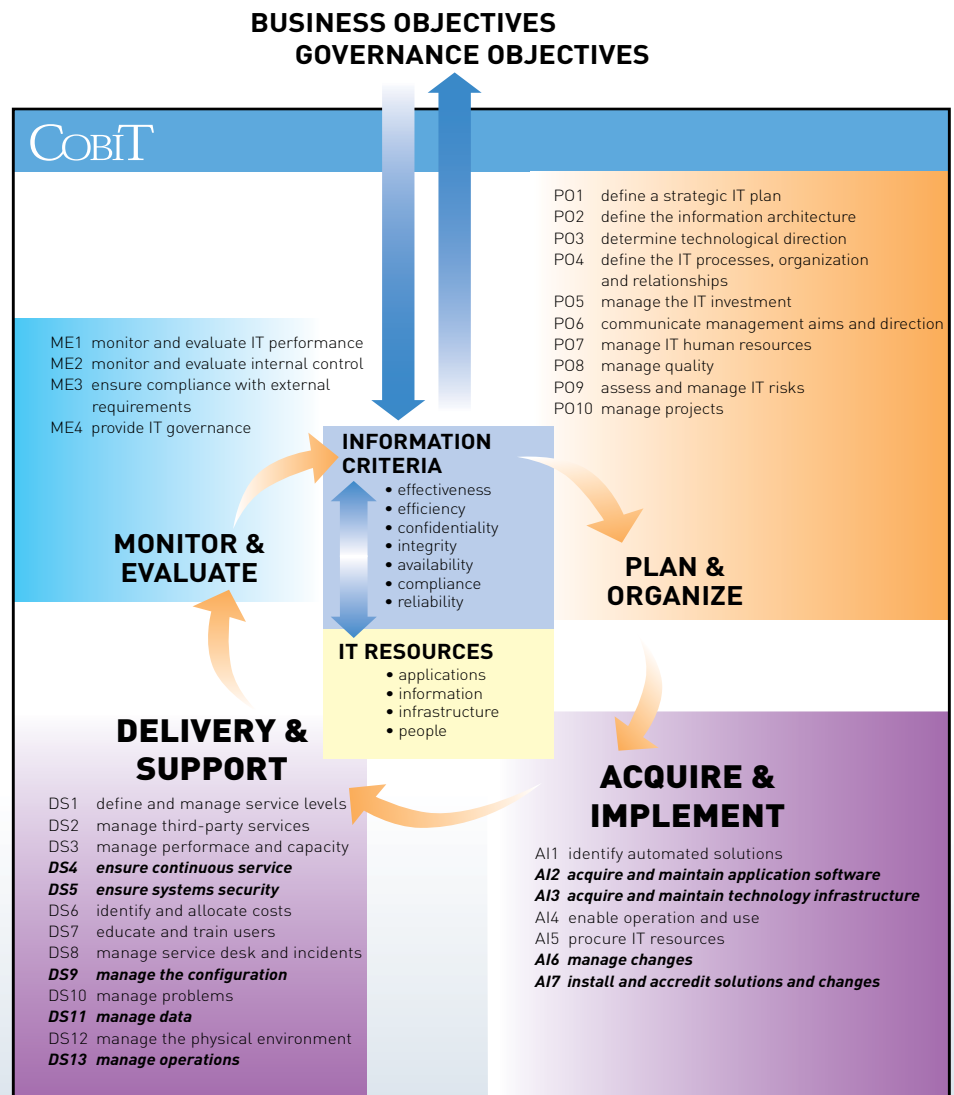
COBIT is the IT-specific aspect of COSO's control framework. Tripwire configuration audit and control solutions support many elements of the Acquire and Implement (AI) and Delivery and Support (DS) guidelines of COBIT. The following are just a few of the COBIT recommendations where Tripwire excels as the solution.

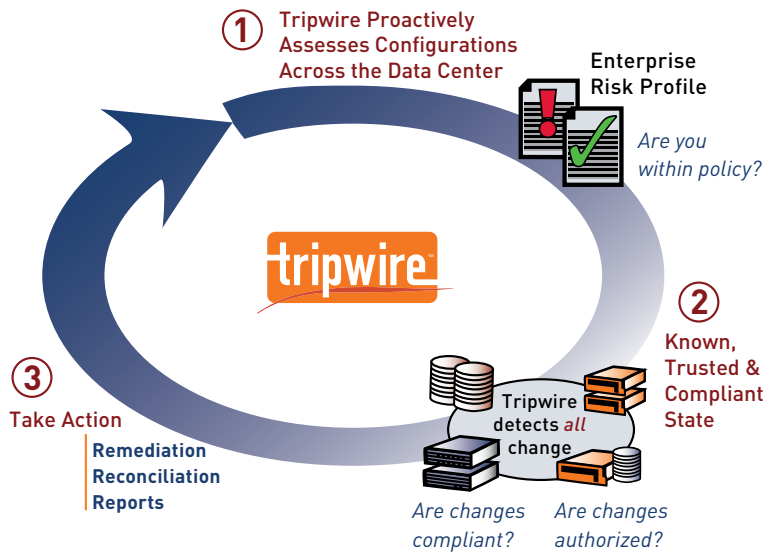
- **Conduct regular vulnerability assessments.** Tripwire leverages industry standards and frameworks, such as COBIT, to automatically assess configurations and determine the degree of risk.
- **Regularly test configurations, systems and processes.** Tripwire tests system settings against established baselines and standards, identifying areas where controls are configured incorrectly or non-existent.
- **Document and implement detective controls.** Tripwire is commonly used to monitor the configuration, applications, and underlying OS of security software and devices in order to detect and report change. In this way, Tripwire provides independent validation that security applications and their configurations have not been compromised or changed without authorization.
- **Document change management workflow approval processes.** Tripwire enables user-scheduled integrity checks to monitor files and their attributes, comparing them against the baseline. Changes are immediately pinpointed and appropriate IT staff can be notified by email or pager.
- **Document and implement preventative controls procedures.** Tripwire validates that all changes are tracked, synchronized with documentation, and applied consistently across the appropriate systems.

Sustaining Compliance with Tripwire Software

One of the leading causes of security breaches, loss of data, and regulatory non-compliance are improperly configured systems. That is why it is so important to keep IT systems in a known, trusted and compliant state. Given today's complex infrastructure it requires a solution that can automatically audit change and manage the assessments of configurations across the data center. To be truly effective, controls must cover the entire enterprise, monitoring activity occurring on servers, network devices, databases, directories, and virtual environments.

Tripwire Enterprise plays a vital role in sustaining compliance by helping IT management validate compliance with these requirements by delivering out-of-the-box configuration assessment and change audit capabilities for the data center. Tripwire leverages industry benchmarks and frameworks such as COBIT to automatically assess configurations for SOX compliance and determine the degree of risk. Then we help you continuously maintain a known and trusted state through ongoing, tunable change detection.





- Tripwire Enterprise scans the entire IT infrastructure's configuration settings, providing a baseline configuration known state.
- It then analyzes all configuration settings and identifies the difference between the current state and an established known good or compliant state, then provides an enterprise risk profile.
- Using policy-driven capabilities, Tripwire enterprise detects all change as it occurs, no matter the source, and without the need to re-scan the entire system. Those changes are then assessed for policy and process compliance.
- Changes that put the system out of policy compliance are automatically escalated so immediate action can be taken.

Continuous Compliance, Reduced Audit Costs

Spend Less Time and Money

Tripwire Enterprise enables you to obtain the proof required to verify compliance with a single, verifiable audit trail. It's sophisticated reporting and automatically generated audit reports gives auditors the

information required to complete annually required audits. This provides important insurance against the financial impact of fines, plus reduces the resources required for audit preparation and manual audit testing efforts.

Reduce Risk with Visibility to all Change

While traditional change and configuration management tools provide a process for orderly change, they don't guard against human error or unauthorized changes made by either staff or intruders. Tripwire enterprise monitors and reports on every change made across the data center regardless of source, detecting unauthorized change and non-conforming configurations to proactively discover and manage security and compliance exposure.

Continuously Validate Your Process

Tripwire Enterprise combines change auditing and configuration assessment, automatically reporting configuration settings against policy to help you achieve continuous compliance. Tripwire's powerful approach leverages industry frameworks from COBIT. This includes Configuration Assessments for SOX, enabling automatic, out-of-the-box policy compliance testing. Tripwire's unique and comprehensive approach helps ensure your systems achieve and maintain a known and trusted state.

"With Tripwire, we could immediately see that only the things we expected to change, actually were changed. This opened up new possibilities for managing change in a more organized way, which led to the use of Tripwire as part of our formal change management process."

— John Francis
Vice President,
Mercantile Bankshares Corp.

Fitting Tripwire into Your Sarbanes-Oxley Readiness Strategy

| COBIT CONTROL OBJECTIVES | TRIPWIRE PRODUCTS | TRIPWIRE SERVICES |
|---|-------------------|-------------------|
| ACQUIRE AND IMPLEMENT | | |
| AI2: Acquire and Maintain Application Software | | |
| AI2.3 Application Control and Auditability | ✓ | ✓ |
| AI3: Acquire and Maintain Technology Infrastructure | | |
| AI3.2 Infrastructure Resource Protection and Availability | ✓ | ✓ |
| AI3.3 Infrastructure Maintenance | ✓ | ✓ |
| AI6: Manage Changes | | |
| AI6.2 Impact Assessment, Prioritization and Authorization | ✓ | ✓ |
| AI6.3 Emergency Changes | ✓ | ✓ |
| AI6.4 Change Status Tracking and Reporting | ✓ | ✓ |
| AI7: Install and Accredite Solutions and Changes | | |
| AI7.6 Testing of Changes | ✓ | ✓ |
| AI7.9 Post-implementation Review | ✓ | ✓ |
| DELIVERY AND SUPPORT | | |
| DS4: Ensure Continuous Service | | |
| DS4.5 Testing of the IT continuity Plan | ✓ | ✓ |
| DS4.8 IT Services Recovery and Resumption | ✓ | ✓ |
| DS5: Ensure Systems Security | | |
| DS5.3 Identity Management | ✓ | ✓ |
| DS5.4 User Account Management | ✓ | ✓ |
| DS5.5 Security Testing, Surveillance and Monitoring | ✓ | ✓ |
| DS5.7 Protection of Security Technology | ✓ | ✓ |
| DS5.8 Cryptographic Key Management | ✓ | ✓ |
| DS5.9 Malicious Software Prevention, Detection and Correction | ✓ | ✓ |
| DS5.10 Network Security | ✓ | ✓ |
| DS5.11 Exchange of Sensitive Data | ✓ | ✓ |
| DS9: Manage the Configuration | | |
| DS9.1 Configuration Repository and Baseline | ✓ | ✓ |
| DS9.2 Identification and Maintenance of Configuration Items | ✓ | ✓ |
| DS9.3 Configuration Integrity Review | ✓ | ✓ |
| DS11: Manage Data | | |
| DS11.6 Security Requirements for Data Management | ✓ | ✓ |
| DS13: Manage Operations | | |
| DS13.3 IT Infrastructure Monitoring | ✓ | ✓ |
| DS13.4 Sensitive Documents and Output Devices | ✓ | ✓ |
| DS13.5 Preventive Maintenance for Hardware | ✓ | ✓ |

"Without Tripwire, Cascade Microtech would have had to undergo an extensive and time-consuming sampling exercise, costing time and money to request, gather and compare change request logs. Tripwire's ROI is there several times over."

— Protiviti On-site Auditor

Services to Help Organizations Develop Sustainable Compliance Processes

Tripwire Professional Services is available to help you get the full impact and benefit of a Tripwire configuration audit and control solution, the key component to meeting compliance regulations. Contact Tripwire Professional Services today to ensure your SOX compliance efforts and audit process are successful.



www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA