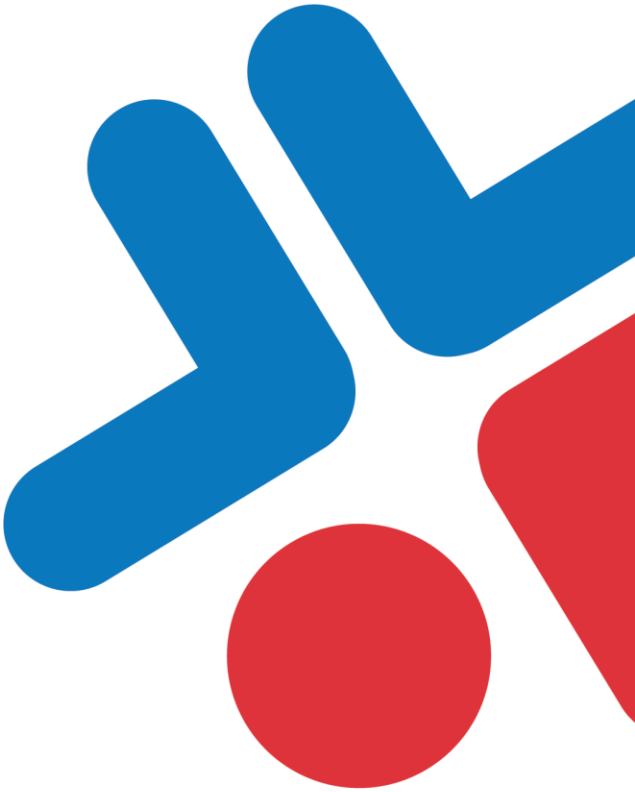
netwrix
#1 for change auditing

2014 State of IT Changes Survey Results



netwrix
#1 for change auditing

2014 State of IT Changes Survey Results

In 2014, change is the only constant. Changes to critical IT systems are a daily part of any IT organization's ability to meet the constant barrage of requests for improved, faster and more efficient services. It's also a foundational part that causes system downtime, security breaches, internal and external threats and decreases in operational efficiency.

Without a means to track what has changed, an IT organization has little ability to know what change was the root of a data breach or what caused a system to stop functioning properly, let alone be able to know exactly what to revert to fix the problem. Many organizations manage major changes by using everything from a spreadsheet to more advanced change management solutions. Other organizations choose to utilize nothing more than raw log data as a means to have some level of insight into changes. Those organizations that only rely on change management processes or solutions are allowing their IT organization the ability to simply bypass the change management in place and make changes not logged and tracked.

Organizations taking IT changes the most seriously are utilizing change auditing solutions that automatically monitor changes to critical systems, notify IT personnel, and provide historical reporting. Change auditing is a foundational part of any IT organization's security plans, change management processes and compliance programs. Companies that utilize some form of change auditing gain visibility into when changes were made, what specifically was changed and by whom.

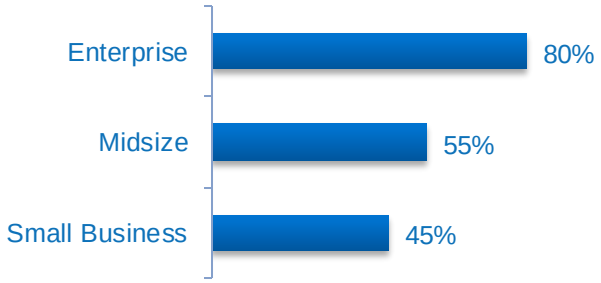
Netwrix surveyed 577 IT professionals about the state of changes made by IT to provide an idea of how organizations today see the impact of changes made, the use of change auditing and the methods and processes intended to maintain security and system availability. Also this survey is focused on whether the change management and auditing is truly useful by asking members of IT organizations, if they are making changes without knowing their peers, circumventing the change management, auditing processes and systems that are in place. Additionally, the survey covers the kinds of changes IT is making and the impact they have.

Our goal in this report is to provide multiple perspectives for different IT organizations, so we have chosen to break down the responses by organizational size, industry vertical and size of IT organization.

Survey Highlights

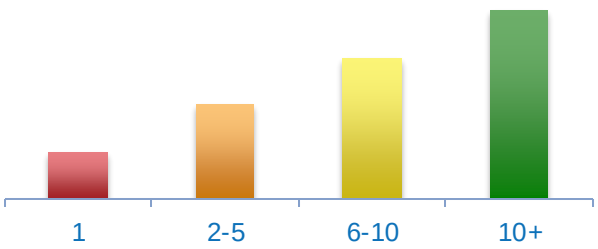
Who is the most serious about tracking IT changes?

When asked whether change management process controls were in place for IT changes, Enterprise organizations with more than 1000 employees claimed the highest level of processes, systems and controls in place to manage and audit IT changes, weighing in at **80%**. This trend of the Enterprise taking IT changes and their impact seriously follows through most of the survey.



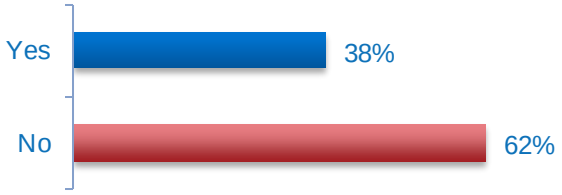
Is it organization size or IT organization size?

When looking at how seriously organizations of various sizes take IT changes, a higher correlation exists between the **number of IT staff in an organization** and their position on managing and auditing IT changes, especially when compared to the size of the organization itself.

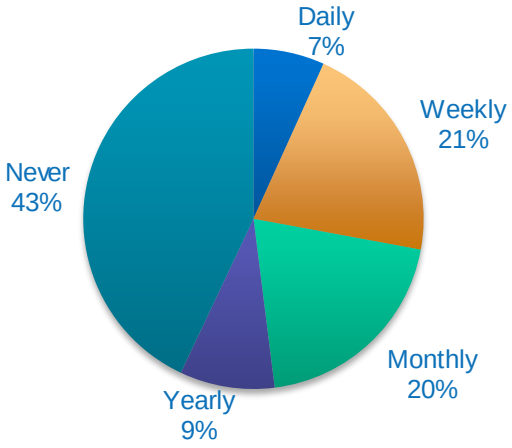


Are organizations auditing changes to IT systems?

While at face value it seems that organizations take IT changes seriously, when asked if they have any system in place to audit changes to critical IT systems, only **38%** responded positively. We dug deeper and found that many organizations answering YES considered just having system log data enough to answer affirmatively.



Who's making undocumented changes?



Surprisingly, when asked about making changes that no one else knew about, **57%** admitted to making continual periodic changes *without* documenting the changes.

Respondent Demographics

Organization Size

We grouped organizations by size using Gartner's definitions[1] of small business (1-100 employees), midsize enterprises (101-1,000 employees) and enterprise business organizations (1,001+ employees). Figure 1 shows the breakdown of organization sizes responding to this survey.

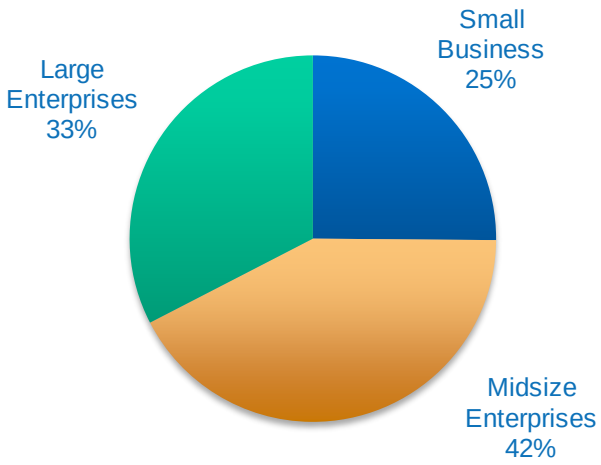


Figure 1: Respondents by Organization Size

[1] http://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses

Industry Vertical

We received survey responses from IT staff working in 24 different industries. Figure 2 shows the breakdown of the industries most represented with those least represented grouped together.

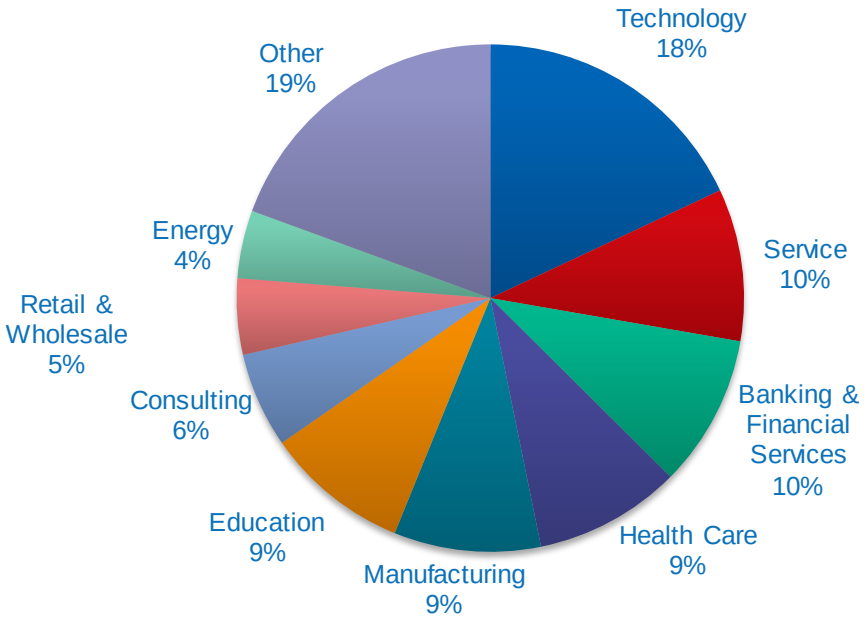


Figure 2: Respondents by Industry

IT Organization Size

IT staffs vary size from one to one hundred (and everything in between). IT staff size responses in this survey were no exception, as shown in Figure 3.

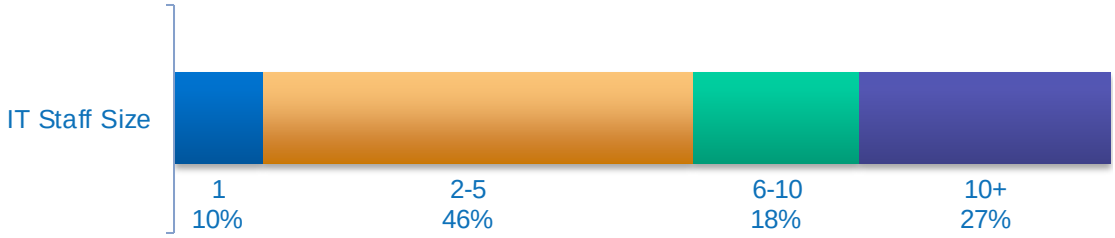


Figure 3: Respondents by IT Organization Size

Respondents cited varying IT staff sizes in conjunction with their organization size, as shown in Figure 4.

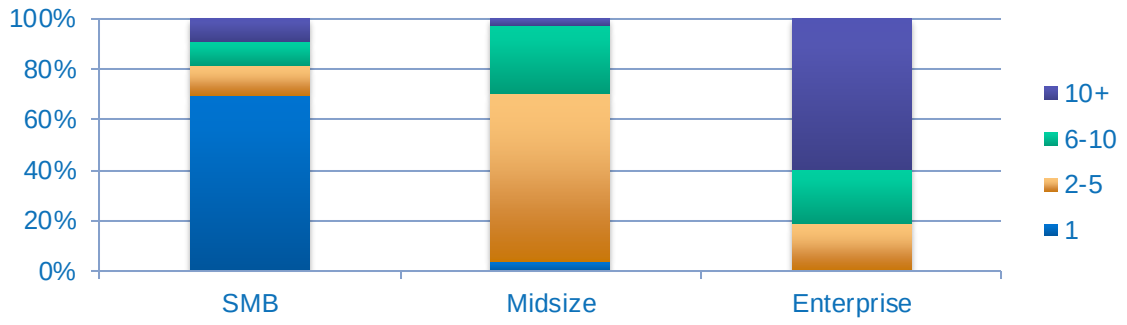


Figure 4: Size of IT Staff by Organization Size

Survey Responses

The focus of this survey was to find out whether IT organizations are managing and auditing changes made within IT infrastructure, what kind of impact do these changes have and how IT pros can manage and audit configuration changes.

Change Management: Who's Doing it and Why

IT is using some form of change management controls

On an average, **60%** of organizations claimed to have some kind of change management controls in place, as shown in Figure 5. It's no surprise to see that SMBs have the least handle on change management leaving them exposed to changes that may influence security or system downtime. Midsize organizations have little more than their SMB counterparts. Given the higher percentage of a larger number of IT staff, midsize IT organizations are even more susceptible to problems arising from IT changes.

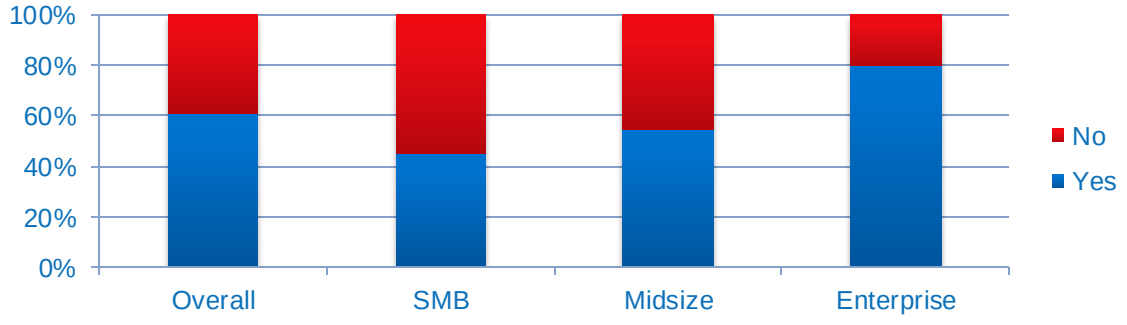


Figure 5: Does IT have change management controls in place?

IT is documenting their changes

Not surprising, most organizations are making some effort into documenting changes with the average around **80%**, as shown in Figure 6.

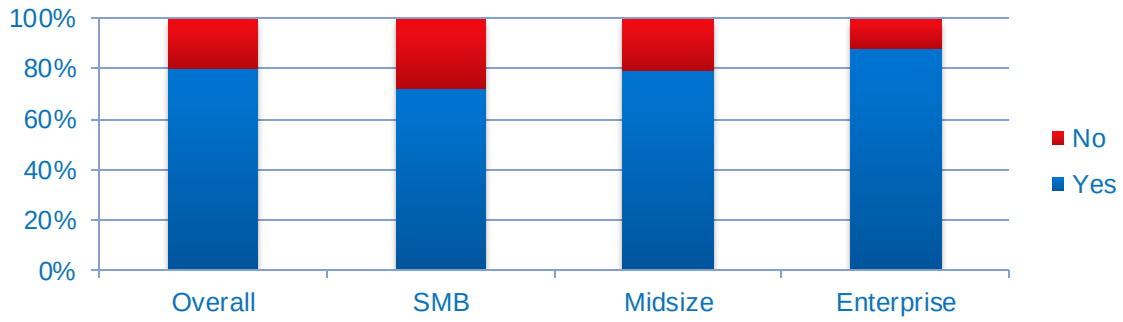


Figure 6: Are IT organizations documenting changes? (By organization size)

Digging a bit deeper into the data, we found that **40%** of those stating they did not have change management process controls in place are still documenting changes.

When looking at the size of the IT department, rather than the organization size as a whole, we found a far more distinctive trend in the attitude towards documenting IT changes, as shown in Figure 7. This should come as no surprise, that organizations with larger sizes try to document changes made in order to keep IT staff informed of what is going on, whereas IT pros in smaller organizations mostly keep everything in mind.

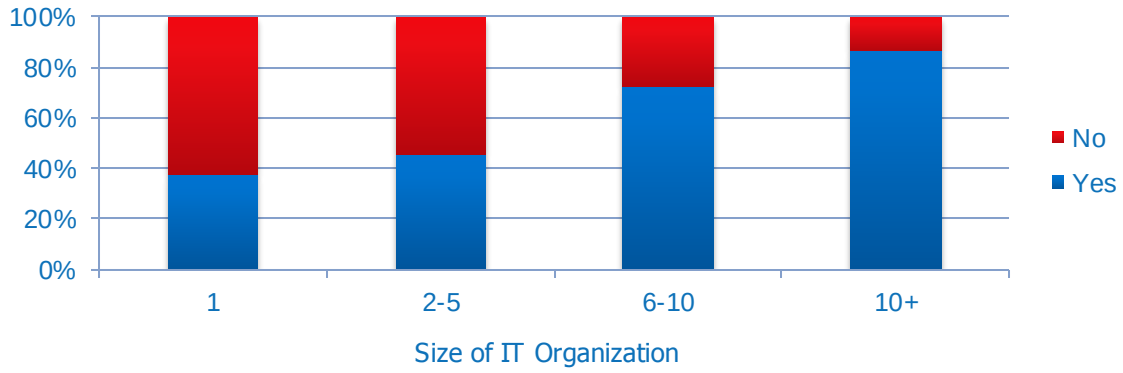


Figure 7: Are IT organizations documenting changes? (By IT organization size)

How frequently is IT making changes that impact security?

It's clear to see the need for tracking changes when you consider that **40%** of all organizations surveyed are making changes to IT either daily or weekly, as shown in Figure 8, this activity definitely impacts companies' security.

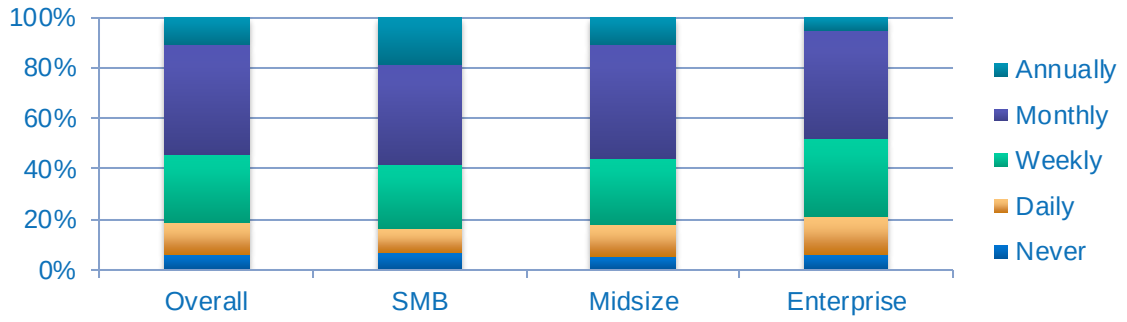


Figure 8: Breakdown of the frequency of changes impacting security

How frequently is IT making changes that impact performance or service uptime?

Similar to changes impacting security, organizations make frequent changes, this time impacting system performance or service uptime. Overall, organizations are in line with security-related changes with nearly **42%** making changes either daily or weekly, as shown in Figure 9. Surprisingly, despite the fact that these changes would be far more noticeable by the organization as a whole, and that enterprise organizations have many more users impacted by system downtime, nearly **52%** of enterprises make these kinds of changes daily or weekly.

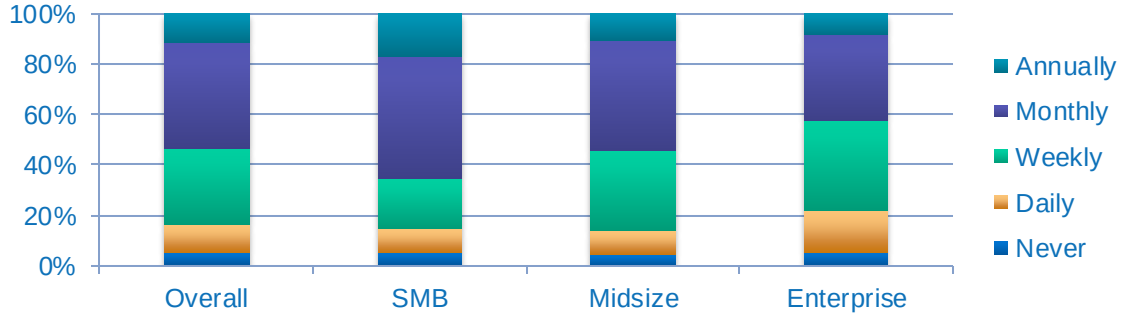


Figure 9: The frequency of changes impacting performance and uptime

Change Auditing: Putting Change Management to the Test

We wanted to validate the usefulness of the change management systems and processes utilized by IT organizations by testing whether they are validating the use of those systems and processes by use of a change auditing method or solution.

Having a system to manage and track changes in place and utilizing it is a great first step, but without a system in place to audit all changes made, there is no way to verify whether the change management processes are being used. Change auditing allows organizations to review changes as well as ensure that all changes are documented accurately.

IT isn't auditing their own changes

While the majority of IT organizations are utilizing some form of change management processes, **62%** of our respondents indicated that they have little or no real ability to audit the changes made, as shown in Figure 10. This leads to missed changes, an inability to meet compliance objectives and results in security gaps. This inability lessens as the organization size grows.

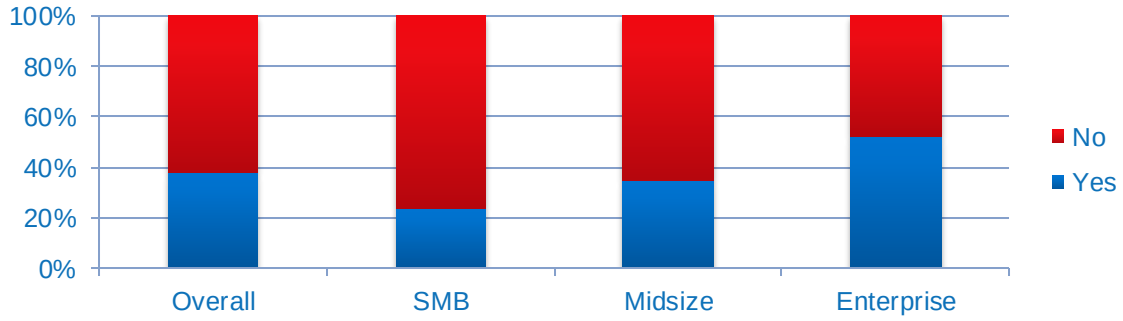


Figure 10: Is IT auditing changes? (By organization size)

Like the documenting of changes, the responses, when looked at through the lens of organization size, produced a far more dramatic increase in the usage of some form of change auditing. From **13%** of SMBs up to **60%** of enterprises use change auditing as a means to validate the changes.

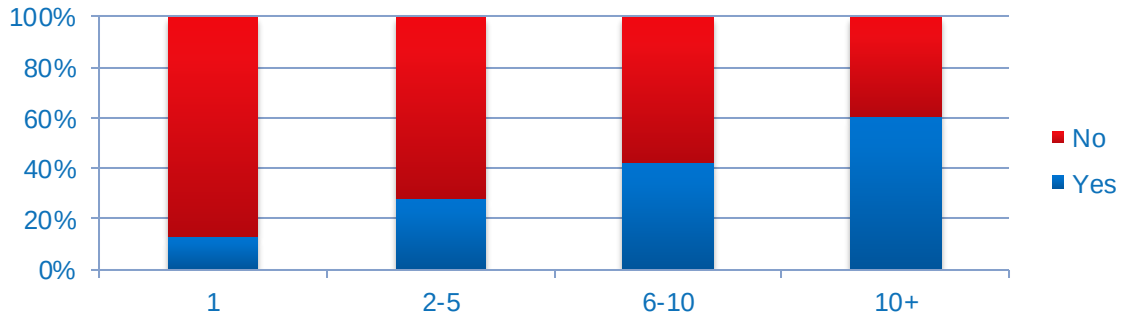


Figure 11: Is IT auditing changes? (By IT organization size)

IT sees Change Auditing in very different ways

Of those that indicated they had a system in place to audit changes, only **23%** had either an audit process or a true change auditing solution in place to validate changes are being entered into a change management solution. As shown in Figure 12, other organizations believe their change management process or solution *is* their change auditing solution (which is a bit like asking the watchers to watch themselves). Others are simply documenting their changes manually, using native event log tools, or nothing at all.

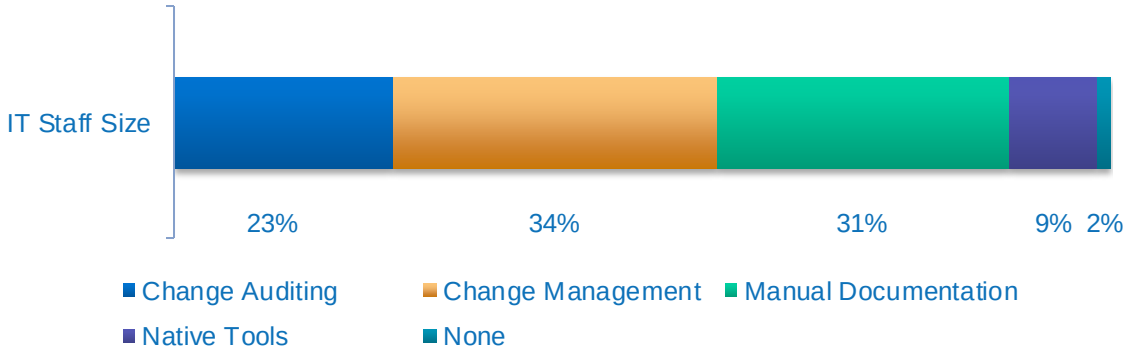


Figure 12: Change auditing solutions utilized

Is Change Auditing Necessary?

The survey has demonstrated that while a vast majority of organizations are employing some level of change management or change documentation, very few are putting that process to the test. So we wanted to know whether organizations had reason to require change auditing. Is every change being documented? Are the changes being made causing security breaches? System downtime? It's the answers to these kinds of questions that help an organization understand whether they need to be auditing IT changes.

IT is making changes to critical systems without documenting

The notion that every change actually goes into the change management solution is put to the test with this question. When asked if changes were made without documenting, on average **57%** of IT organizations are making changes at varying levels of frequency without documenting the change. We saw this same shocking trend across all three organizational size segments with Enterprise being the worst offenders.

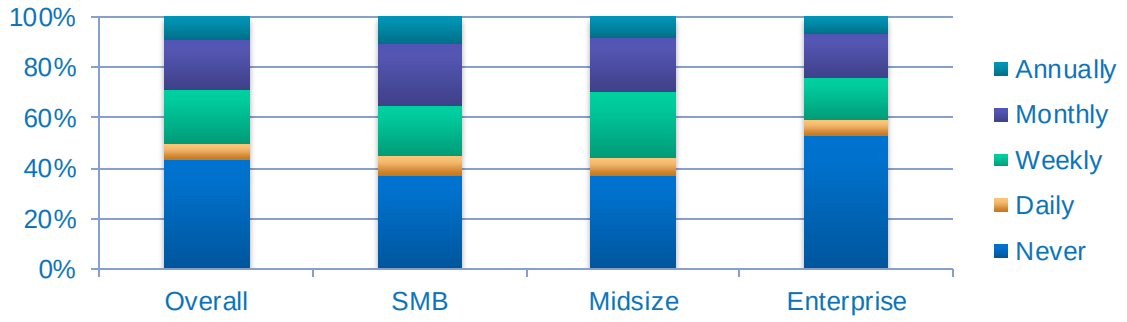


Figure 13: The frequency of undocumented changes

If such a high percentage of IT organizations admit to bypassing their own controls, it becomes imperative to understand whether these undocumented changes are causing harm to the organization as a whole.

IT is making changes that cause service interruption

Nearly **65%** of IT organizations admitted to making changes that caused services to stop. It's surprising to see that, despite the increased focus on managing and auditing changes as organization size increases, the percentage of IT organizations making changes that impact service availability grows up as the organization size increases.

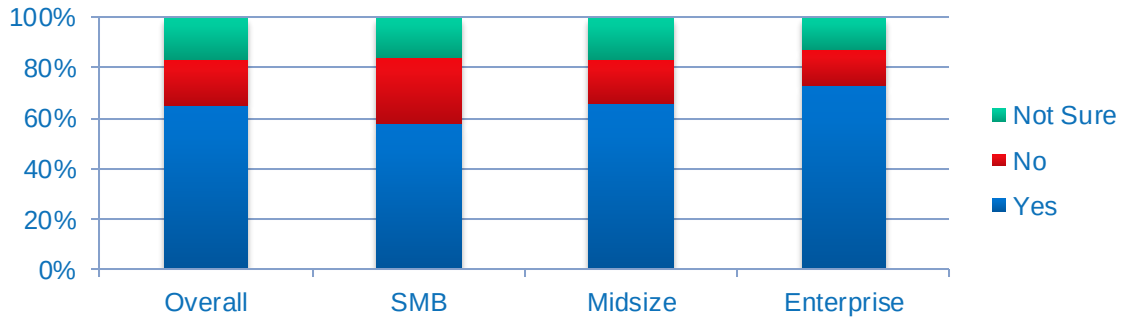


Figure 14: Is IT making changes causing a stoppage in services?

Given over half of IT changes are not being documented, without some ability to know when a change is made and what the change was, IT organizations will be hard pressed to quickly identify the change that caused service interruption.

IT is making changes that cause security breaches

IT organizations appear to be far more serious about changes when it comes to security. We asked if IT organizations had ever made a change that was the root cause of a security breach, an overwhelming **61%** claimed to have never made such a change. SMBs were the most security change-conscious with **67%** of respondents claiming to not having made such a change. Midsize organizations had the largest uncertainty of whether their changes impact security at **29%**, with Enterprises being the worst offender with **17%** of respondents admitting changes were made that caused a security breach.

Figure 15: Is IT making changes that caused a security breach?

Conclusions and Recommendations

When a breach occurs, a system goes down or an auditor shows up, questions are going to be asked. Tough questions like "Who made changes to this system yesterday and what was changed?" IT organizations today have the best of intentions to proactively prepare for such moments. But with so many IT professionals making changes without using the very systems they themselves have implemented, it is going to be nearly impossible for them to provide answers not just to auditors, but to themselves to solve a problem caused by a change.

Without some means of accountability, IT changes will continue in these organizations without any supervision. Having a change management process or system that tracks changes alone won't help; there needs to be an external ability to check that all the changes that have been made are tracked. System logs provide some level of detail, but it is more critical that you have your most important systems monitored for changes where change detail (that may be lacking in logs alone) is provided.

Given that IT organizations are making undocumented changes that impact system availability and security, IT organizations need to take another look at whether their change management needs the addition of change auditing. This will ensure that all changes – both documented and undocumented – are tracked, providing IT the ability to be notified when changes are made, report on and review changes in detail to specific systems at specific times, by specific individuals, and have the ability to find the answers quickly in case a change caused a security breach or service outage.

About Netwrix Corporation

Netwrix Corporation is the #1 provider of change and configuration auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solutions with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have more than 160,000 customers worldwide, and is ranked in the Top 100 US software companies in the 2013 Inc. 5000 and Deloitte Technology Fast 500. For more information, visit www.netwrix.com.

Netwrix Corporation, 20 Pacifica, Suite 625, Irvine, CA

Regional offices: New York, Atlanta, Columbus, London

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261