# BUSINESS CONTINUITY

**Mat Clothier**, *discusses the importance of managing & configuring systems in accordance with SOC 2 Type 2*

**By managing configuration drift effectively, businesses can ensure their estate is prepared for any unforeseen changes in these environments**

**The demand for high-level security within organisations has substantially increased as the technology industry continues to expand. Despite the development of security measures within applications and systems, some of them are yet to be fully protected from viruses and cyberattacks. To ensure businesses maintain the privacy and security of their data, it is important to continually monitor the storage of their information – keeping it safe and taking any necessary precautions to prevent such breaches.**

Auditing systems is a great way for organisations to keep their systems in check and monitor for upcoming updates and compliances. As the need for security increases, so does the number of auditing software available – some valuable and some not. When auditing their estate (servers, desktops, laptops, network infrastructure *etc*), the most important aspect organisations should check is that they are complying with the latest industry regulations – and with these changing regularly, they must be continually monitored. An easy and reliable way to ensure this is by running a SOC 2 Type 2 report – these are especially useful to companies who use third-party services, such as the Cloud.

A SOC 2 Type 2 report runs and provides an in-depth analysis and thorough examination of a company's security status, including a report on its vulnerabilities and threats. It also offers recommendations on how to improve any systems that are lacking or falling behind on current security measures/protocols. By running a Type 2 report, organisations can gain a SOC 2 certification, which essentially demonstrates that they are running on the most beneficial and efficient systems while keeping their data stored correctly and safely. This certification also proves that the organisation is protecting both the business and its customers from stolen information and bad actors.

Configuration management tools (also known as CM tools) are software tools that assist in the management and maintenance of an organisation's technological infrastructure. These tools typically provide a way for businesses to monitor information and updates within all systems of their estate – for instance, when new regulations, updates or software versions arise that must be complied with. Such tools allow businesses to stay one step ahead and always be prepared for any upcoming changes they need to make. This allows businesses to create a security development plan and allocate time, money and resources to these adjustments. Staying ahead of the changes allows businesses to remain secure and minimise time spent playing catch up with developing software – potentially leaving them vulnerable to an attack while their efforts are focused on making the required updates.

Having CM tools in place helps organisations comply with regulatory requirements and assists in achieving optimal operational efficiency. Certain tools also offer automation services that allow businesses to automate tasks such as rolling out new applications, systems or updates – keeping them ahead of the game and all systems in the best state, reducing the risk of gaps appearing in technology, and therefore increasing the level of security.

Configuration management tools provide great benefits to organisations and can be seen as essential for maintaining business continuity while ensuring compliance with regulations. The primary benefit is that they automate the process of setting up, configuring and maintaining IT systems, while reducing the efforts of employees so their time can be focused elsewhere.

It is becoming increasingly common to see in the news that companies and organisations of all sizes are suffering from cyberattacks and security breaches, with sensitive customer data always at the forefront. According to the Cyber Security Breaches Survey 2022, almost a third (31 percent) of businesses reporting attacks were targeted at least once a week. With these ever-occurring incidents, it is no wonder that more businesses are looking to ensure their own cybersecurity practices are up to date and fully compliant with the latest rules and regulations.

Mishandled data can result in higher vulnerability within organisations, in turn leading to the theft of data and the potential for ransomware and other malware attacks. As previously discussed, one way in which companies can reduce the opportunity for security breaches is by achieving SOC 2 compliance.

SOC 2 provides an assurance to organisations that they have implemented the necessary security controls in order to protect not only their own but customers' personal data too. This certification is becoming progressively important for businesses in the digital age, as customers become more aware of the risks of sharing their personal information online. By proving their security through compliance, companies can provide peace of mind to their customers, allowing trust to be built.

There is a number of benefits that come with achieving SOC 2 compliance, the most important being the reduction of vulnerabilities to cyber-attacks, and the overall building of a more reliable and secure infrastructure. Additionally, it demonstrates to customers that the organisation in question takes its data security seriously and is committed to protecting its information. This can help to build trust and confidence in its brand. It can also give a competitive advantage over other businesses that have not yet achieved compliance; proving to their customers their ongoing dedication to security. Finally, it can help companies to streamline their internal processes and ensure that everyone in the business is aware of and adhering to best practices when it comes to data security.

AS THE SECURITY NEED INCREASES, SO DOES THE NUMBER OF AUDITING SOFTWARE AVAILABLE

Achieving SOC 2 compliance isn't an easy task, but it's well worth the effort for businesses who want to show their commitment to safeguarding their customers' data. Not only that but actually protect their business from bad actors with malicious intent.

Through countless updates and CM tools it can be difficult for organisations to keep up, and if businesses start to fall behind this is when configuration drift can occur.

Configuration drift happens when a company's systems gradually change over time, often without being noticed and leading to them becoming more and more difficult to maintain. This can result in higher operational costs and greater gaps in security, so it is important for businesses to regularly monitor for updates – ensuring they do not drift away from their optimal and most secure states.

Regular monitoring allows organisations to catch any issues early on and make any necessary adjustments before they cause larger problems or become costly to fix. It also encourages systems to operate in the most efficient and secure way – and the way they are intended to. Additionally, with many teams being asked to do more with less, these automated tools are an easier way for employees to monitor the changes rather than finding them manually. With potential personnel or role changes frequently happening this ensures continuous monitoring for compliance, regardless of who is currently in post. It also reduces the amount of valuable employee time spent on checking for and completing updates.

Configuration management tools play a large part in avoiding configuration drift, this is because they allow organisations to monitor possible drifts and

▶

plan ahead. These tools compare the changes in a business' systems and environments over time and provide visibility and control of their configuration flaws, allowing them to proactively act on misconfigurations in a calculated and thoughtful manner.

## SOC 2 CERTIFICATION SHOWS A BUSINESS IS RUNNING THE MOST EFFICIENT SYSTEMS

Controlling configuration drift over time can prove beneficial for any organisation as it prevents unnecessary changes to the technological infrastructure and makes businesses more secure from outside threats. It also allows the business to adapt to changing conditions and be prepared for them when they inevitably happen. Managing the ever-growing list of devices, software and company-specific protocols can be a difficult and lengthy task, not to mention ensuring they also align with industry standards.

However, by proactively dedicating time to configuration management, organisations can prevent drift and provide a stable foundation for their infrastructure, including their applications and systems. By managing configuration drift effectively, businesses can ensure that their estate is futureproofed and prepared for any unforeseen changes in these environments.

SOC 2 Type 2 reports are continuously generated over a period of time rather than a one-off check, therefore monitoring potential configuration drift over time and proving that controls are followed routinely and used effectively making the estate more reliable and secure. This will in turn reduce the likelihood of any unwanted cyber-attacks or threats.

Organisations that adopt SOC 2 Type 2 compliance are taking the necessary steps to ensure their systems are in a secure state and their data is stored safely – protecting both the business and their customers. Monitoring over time can help organisations identify any potential security flaws and make the appropriate changes to mitigate any risks. Through utilising CM tools, businesses avoid potential configuration drift, ensuring that all systems remain in a secure and compliant state. By taking the necessary precautions, organisations can maintain their SOC 2 Type 2 compliance and ensure their data is secure.

While compliance with rules and regulations is one of the more important reasons to keep software and a company's entire IT estate up to date, there are many other reasons to stay ahead of the updates (usability and speed of applications/systems, for example). By putting in the work and protocols before problems arise, organisations are taking active steps to protect themselves and their customers as well as allowing their employees to be more streamlined and efficient. The process of checking for compliance doesn't need to be hard and cumbersome, if done routinely and with the right tools, it should feel like a simple routine check. The ongoing simple checks and implementation where appropriate will save companies time, money and a damaged reputation due to non-compliant software. This type of damage is avoidable with a little foresight and consideration ●

**Mat Clothier** is CEO and Founder of Cloudhouse.

**Configuration management tools play a large part in allowing organisations to monitor possible drifts and plan ahead**