RingCentral

Compliance in communications: what it is and why it matters

How to get your bearings among ISO, GDPR, HITRUST and all the other acronyms

Table of contents

Introduction

Cyber attacks have always presented a huge challenge for businesses, but the rise of remote and hybrid working in recent years has significantly increased the risk.

With employees working at home on public networks, via their own personal devices with apps that don't pass the same levels of scrutiny they might in an enterprise environment, businesses must be aware of the vulnerabilities that can come with more flexible working.

Now, as even the most forward-thinking businesses find it difficult to oversee and manage their security risks, it's become more crucial than ever for organisations to invest in more efficient security.

This guide takes a detailed look at:

- How the rise of hybrid work impacted the cybersecurity landscape
- What compliance means and why it matters
- What certifications and attestations to look out for

Flexible hybrid work comes with higher cybersecurity risks

While hybrid work comes with so many advantages, it also presents huge levels of risk for your business. According to TechTarget, there are several critical remote working cyber risks in the UK including the following:

- Shadow IT
- Unsecured and vulnerable networks
- Less oversight
- Growing attack surfaces
- Insufficient data practices
- Unsecured and vulnerable hardware
- Vulnerability to phishing attacks
- Susceptibility to webcam hacking
- Misconfigurations in the public cloud

Managing all of these vulnerabilities is a lot for any business to handle. The good news is, using cloud solutions can make improving your security easier, as long as you can choose the right cloud vendors and ensure the solutions are secure. Businesses today must take the time to ensure they've partnered with the technology vendors that put in the work and continuously improve their security capabilities.

Compliance: why it matters

Simply put, compliance means conforming to a set of rules, specifications, policies, standards or law. Depending on your industry, and the territories you operate in, you'll need to adhere to different principles and policies. But compliance, in an increasingly digital and therefore, unpredictable working landscape, has become more and more important. Adhering to compliance, while it might seem daunting, helps to prevent businesses from foul play, protects your business, your employees and your customers, and helps build trust.

Meeting global standards for security and privacy

Finding cloud vendors might seem easy. And with critical business decisions piling up on a daily basis, facing the huge challenge that is compliance, is daunting. But taking the easy route, or following the crowd when it comes to choosing your cloud communications vendor, could be a huge mistake - namely because of your compliance. Businesses must choose partners and vendors that can demonstrate their compliance in all of the countries your business operates in.

The following certifications attest to the maturity of a vendor's processes and programmes against the highest global standards. They might be what you need to look for, depending on how sensitive your data is, and the countries you conduct business in.

ISO 27001 certification

What it is: The ISO/IEC 27001 is the globally recognised standard for information Security Management Systems (ISMS) and their requirements. It allows organisations of all sizes and industries to safely oversee the security of their sensitive data, whether that's financial information, employee data, or intellectual property.

What it means: This certification recognises that the vendor has designed and implemented a set of controls and measures to effectively manage risk and achieve compliance continually to protect customer information and data. The certification also demonstrates that the vendor has a robust security programme with rigorous management activity and technical controls to address leading Confidentiality, Integrity, and Availability (CIA) principles of Information Security.

ISO 27017 certification

What it is: The ISO/IEC 27017 certification provides a set of guidelines for IT security controls. These apply to the use of cloud solutions and services specifically and implementation guidance is outlined for appropriate controls specified in ISO/IEC 27002. This global security standard necessitates best-practice guidance on controls and implementation for both cloud service providers and their customers.

What it means: This certification demonstrates that the company extends its disciplined Information Security Management System (ISMS) to the operation of its cloud services. It shows that the vendor applies strict controls policies to secure access its services.

ISO 27018 certification

What it is: This certification centres on establishing commonly accepted controls and guidelines and implementing measures that best protect Personally Identifiable Information (PII) for the public cloud computing environment.

What it means: The ISO/IEC 27018 certification indicates that a specific vendor has a commitment to the privacy of its customers' data. It also demonstrates that the vendor, acting as a processor of its customers' PII data (Personally Identifiable Information), has implemented sufficient controls for protecting PII.

SOC 2 attestation

What it is: SOC, here stands for Service Organization Controls, and the SOC 2 attestation is the American Institute of CPAs (AICPA) reporting standard that defines the criteria for managing and processing customer data. Many organisations, but specifically SaaS businesses choose to adhere to stringent information security procedures, the SOC 2 attestation is a third-party audit that assesses and certifies their compliance.

What it means: Vendors that achieve the SOC 2 attestation have undergone a stringent audit that centres on the controls around the availability, security and confidentiality of customer data.

SOC 3 attestation

What it is: The SOC 3 attestation, unlike the SOC 2, is a public report. That simply means, where the SOC 2 might only be shared with customers or those under NDA, the SOC 3 is a report that can be shared freely or published online. The report gives transparency around an organisation's internal controls over security, availability, processing integrity, and confidentiality.

What it means: The SOC 3 attestation provides assurance about the controls at a service organisation relevant to security, availability and confidentiality. Those who consume the report do not need the in-depth knowledge to make effective use of a SOC 2 report.

STIR/SHAKEN

What it is: STIR/SHAKEN is an acronym for Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted information using tokens (SHAKEN). STIR/SHAKEN is essentially a framework of interconnected standards that enables call recipients to verify caller ID.

What it means: STIR/SHAKEN enables calls that travel through interconnecting telephone networks to be 'signed' as verified by the original carrier, and validated by other carriers before reaching the call recipient. Phone vendors that use this framework protect their users from the risks of unauthorized people joining or intercepting a call.

HIPAA attestation of compliance

What it is: Healthcare and technology are inseparable, but these days, healthcare institutions must comply with a stringent set of regulations. In this case, the Health Insurance Portability and Accountability Act (HIPPA), is a prevalent attestation in the USA.

What it means: While HIPAA doesn't have a presence, or an equivalent in the UK, organisations that do business in the USA still need to adhere to the regulations outlined by HIPAA. Vendors that abide by the HIPAA attestation of compliance, are committed to safeguarding patient or member data, information and healthcare professionals and proved they provide sufficient security protocols to ensure their protection.

HITRUST certificate

What it is: HITRUST is an acronym for Health Information Trust Alliance. It enables businesses of all sectors, but particularly healthcare, to oversee their data, information risk, and compliance.

What it means: Having a HITRUST certificate from the HITRUST Alliance means vendors can display that they have adhered to a standardised framework, giving evidence of their compliance as per HIPAA requirements.

GDPR

What it is: GDPR stands for the General Data Protection Regulation. It was established by the European Union as a data protection law and applies to businesses operating in the EU. The toughest privacy and security law in the world, GDPR outlines regulations on how to collect and process data and aims at protecting the personal data of all EU citizens. Failure to adhere to these privacy and security standards could result in hefty penalties for the businesses that violate them.

What it means: Vendors that prove they comply to GDPR show their commitment to the protection all personal data they store, transfer or process. Since companies are responsible for the protection of their client's data, even when they are processed by a subcontractor, compliance to GDPR is an absolute must for all vendors whose clients do business in the EU.

PCI-certified merchant

What it is: PCI DSS stands for the Payment Card Industry Data Security Standard (PCI DSS). The standard is designed to ensure that businesses processing, storing and transmitting payment card information provide a safe and secure environment.

What it means: Certified organisations commit to a particular way of processing, and storing data related to customer payment cards, and adhere to a number of steps should a security incident occur. For merchants, such as RingCentral, that comply with PCI DSS, it means they abide by a set of principles and guidelines assigned by the PCI standards council when processing customer credit card data.

PIPEDA

What it is: The Personal Information Protection and Electronic Documents Act (PIPEDA) refers to the federal data privacy law for private sector businesses in Canada. Similar to the European Union's GDPR, PIPEDA is a law that regulates the collection, use and disclosure of personal information. Originally brought in in the year 2000, the law was established to ensure businesses foster trust in eCommerce.

What it means: PIPEDA applies to any private enterprise in Canada. Relating to personal information as data obtained as part of commercial activity, the law protects against the unlawful use of personal information. Vendors that comply with PIPEDA show their commitment to personal data privacy.

C5

What it is: The C5 is a government-backed German verification framework implemented by the German Federal Office for Information Security (BSI). The five 'C's stand for Cloud, Computing, Compliance, Controls and Catalog.

What it means: The C5 framework applies to cloud service providers. The C5 certification can be used as a way for them to demonstrate to their users, customers, prospects and stakeholders that they have effective security measures in place to mitigate cyber-attacks when using their cloud-based services.

Building trust in your communications

Businesses today need to have unwavering faith in their communications systems. As organisations navigate the many challenges that come with hybrid and remote working, it's crucial to have a vendor that acts as a reliable partner, prioritising and valuing your security and data privacy as your business grows.

RingCentral is just that. Our third-party attestations, certifications and adherence to global laws and compliance regulations give evidence of our commitment to data security, transparency and privacy. Built on a secure cloud platform, RingCentral meets a stringent set of requirements, meaning our customers can rest in the knowledge that we are delivering high-standard cloud security and ensuring personal information and data remains private.

That means the data of RingCentral users, as well as data being processed through RingCentral services, is secure, private and compliant across message, video, phone and fax. What's more, RingCentral's 99.999% uptime SLA means businesses benefit from the most reliable and secure unified cloud platform.

HITRUST CSF Certified

COALFIRE

PCI DSS COMPLIANT

AICPA SOC 2

AICPA SOC 3

GDPR

CYBER ESSENTIALS PLUS

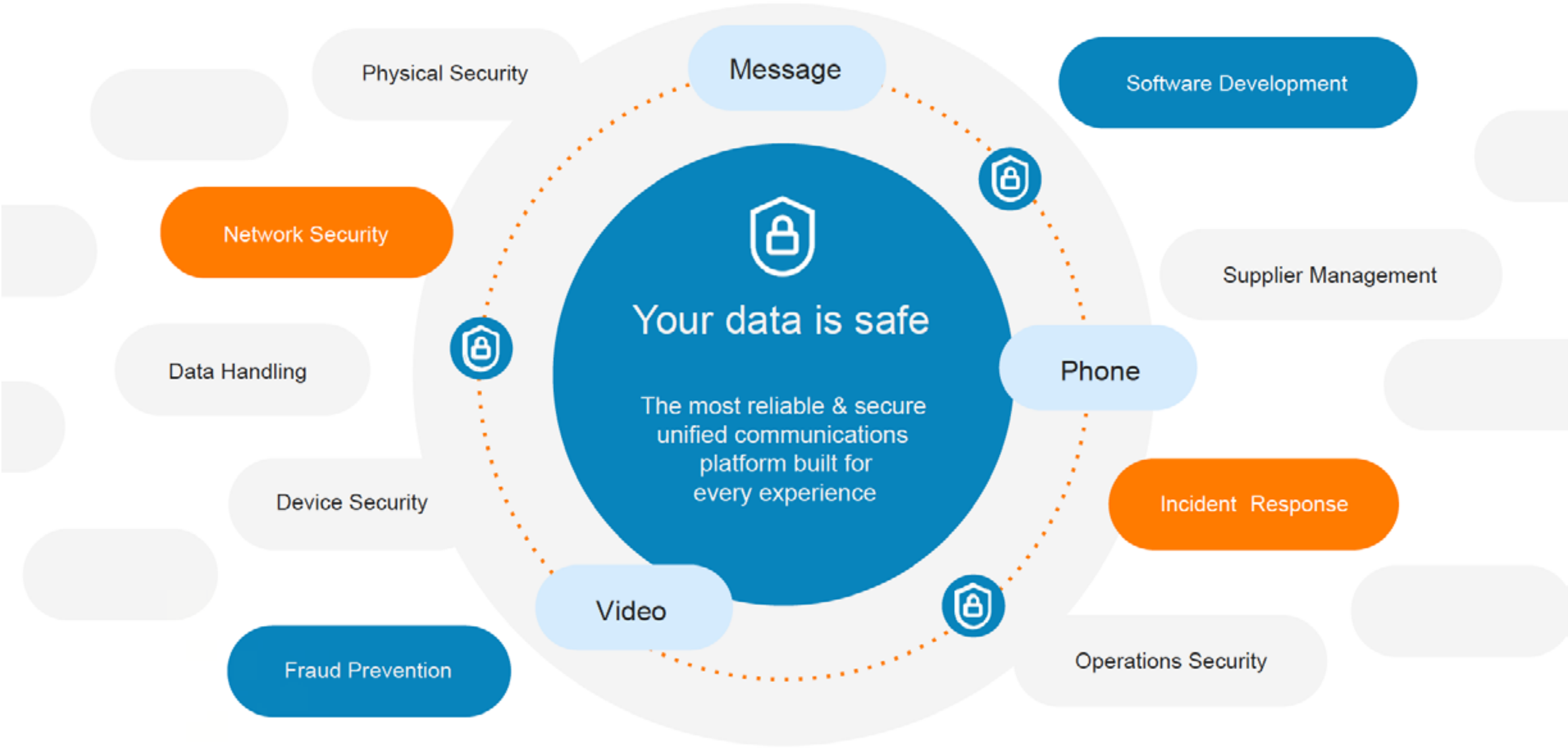
HIPAA COMPLIANT

C5

Beyond compliance

It's important not to forget that compliance is only one aspect of your cybersecurity ecosystem. It's worth assessing what lengths your potential communications partners go to cover information and product security, data privacy and reliability of their solutions.

Besides its high level of compliance, RingCentral also offers best-in-class security, privacy and reliability to keep data safe at every level.



Security

RingCentral's unified communications solution is built with security at the core. With a set of security controls in place, such as single sign-on (SSO), end-to-end encryption (E2EE) and attendee authentication, users put comprehensive administrative controls across messaging, video, and phone, meaning their conversations stay secure, and private. With best-in-class DevSecOps, the platform provides customers with a robust security platform by integrating key security principles from the get-go.

Privacy

Becoming a RingCentral customer, means you'll benefit from our commitment to privacy and transparency. Retaining our customers' trust in data handling practices is a top priority, and so is respecting their data privacy. Our privacy pledge centres around the following core principles:

- Accountability
- Transparency
- Data minimisation
- Privacy by Design and default
- Protection of data subject rights
- Data security
- Safeguards of data transfers

Reliability

We know how important it is to keep operating, and stay connected against all odds. That's why we are dedicated to keeping you open for business wherever and whenever you need to be. Whether it's new offices, different working patterns or a natural disaster, sometimes businesses have to be ready to shift their location. RingCentral customers stay open for business no matter where you work with a 99.999% uptime SLA and redundant internet connections to keep you online during outages, disasters and cyberattacks.

Bottom line

While you may feel you found a great solution to your communication needs when remote working was suddenly mandated, now is the time to question the integrity of your cloud communications vendor.

Whether your team works in-office, remote, or hybrid, safeguarding your communications and keeping your data secure should be a top priority as security breaches continue to sky-rocket. Be sure to review what your suppliers offer in terms of security, reliability, privacy and compliance. Making sure your communications partner ticks those boxes in terms of compliance, and make sure they have the attestations and certifications to prove it, as safeguarding your data and your communications has never been more paramount.

About RingCentral

RingCentral, Inc. (NYSE: RNG) is a leading provider of business cloud communications and contact centre solutions based on its Message Video Phone™ (MVP™) global platform. More flexible and cost effective than the on-premises PBX and video conferencing systems it replaces, RingCentral helps employees communicate across devices from wherever they are. RingCentral offers three key products. RingCentral MVP™ combines team messaging, video meetings, internet phone and other functionalities in a single interface. RingCentral Video™, along with its team messaging feature, enables Smart Video Meetings™. RingCentral Contact Centre™ gives companies the tools they need to connect with customers across channels. These are available on an open platform that integrates with hundreds of third-party apps and makes it simple to customise workflows. RingCentral is headquartered in Belmont, California, USA, and has offices around the world.

For more information, please contact one of our solution experts. Visit ringcentral.com/gb/en/ or call 0800 098 8136.

RingCentral UK Ltd. 85 Uxbridge Road, 4th Floor, Ealing, London, W5 5TH, UK ringcentral.co.uk

03/2023