MARCH 2025

inside zhero

Compliance Game On!

Regulatory versus Framework

Real World Compliance

Cybersecurity Equals Compliance

Compliance Means Business

Compliance Insights from Lucindi

Message from Izak

Welcome everybody to our first spring edition of Inside Zhero this year.

This month, the newsletter is devoted to regulatory and framework cybersecurity compliance. You'll also hear wise words from our amazing Compliance Consultant, Lucindi Strome, citing the fact that compliance is a business imperative.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Compliance Game On!" gives the low down on how businesses need compliance as a survival tool to remain competitive.

The cost of business disruption, productivity and revenue losses, and fines is 3 times the cost of compliance.

"I've come to realise that the ever-evolving nature of cyber threats demands constant vigilance and proactive strategies. We cannot afford to be complacent, as the risks are always shifting and growing. The cost of neglecting cybersecurity is far greater than the investment required to safeguard our digital future. Staying ahead of these threats isn't just a choice. It's a necessity."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

30% discount **cyberzhero542**

COMPLIANCE GAME ON!

Any organisation that handles data – so we are talking about more of them – or has an internet-facing system needs to take cybersecurity seriously. Moving data around or accessing it comes with risks, making organisations vulnerable to cyberattacks. At its core, cybersecurity compliance means following certain rules and standards set by laws, regulatory bodies, or industry authorities. To stay compliant, organisations need to put security measures in place that protect the confidentiality, integrity, and availability (CIA) of their data, whether it's being stored, processed, shared, or transferred. Staying compliant can be tricky because different industry standards often overlap, creating confusion and extra work. Plus, new regulations around data and cybersecurity keep raising the bar. Despite the challenges, cybersecurity compliance is key to an organisation’s success. It’s not just about ticking boxes for regulations. Compliance is about genuinely protecting your organisation from threats like DDoS attacks, phishing, and malware, such as ransomware.

Compliance is critical

No organisation is completely safe from cyberattacks, which is why following cybersecurity standards and regulations is so important. It can play a big role in a business's success, keeping operations running smoothly and security measures in place. Small and medium-sized businesses (SMEs) are often targeted because they're seen as easy pickings. Unfortunately, many don't prioritise cybersecurity, making them more vulnerable to costly attacks. A survey by the Cyber Readiness Institute (CRI) found that only 40% of small businesses put cybersecurity policies in place when remote working increased during the COVID-19 pandemic. Data breaches can seriously damage a company's reputation and finances, and legal action after an attack is becoming more common across industries. That's why compliance is a key part of any organisation's cybersecurity strategy.

Compliance for beginners

For beginners in cybersecurity compliance in the UK, it's important to understand key regulations like the UK GDPR, the Data Protection Act 2018, and the Cyber Essentials scheme, which sets a basic security standard. The UK GDPR and Data Protection Act 2018 outline how personal data should be collected, processed, and stored, ensuring individuals have rights such as accessing, rectifying, and erasing their data. It's also crucial to be aware of data breach reporting requirements, including the 72-hour notification rule. By getting familiar with these regulations, businesses and individuals can build a solid foundation for cybersecurity compliance.

Framework versus regulatory

In the UK, cybersecurity frameworks provide structured ways to improve security, while regulations are legally enforced rules designed to protect sensitive data. Both play a key role in strengthening cybersecurity practices. Cybersecurity frameworks, such as those from the NCSC, offer guidelines, standards, and best practices to help organisations manage risks and improve their security. They provide a structured approach to handling cybersecurity threats and enhancing overall security measures. These frameworks are usually voluntary, meaning businesses aren't legally required to follow them, but they can help with meeting regulatory requirements. In contrast, cybersecurity regulations are legal requirements set by the government or regulatory bodies that organisations must follow. Examples include the Network and Information Systems (NIS) Regulations, the Data Protection Act 2018, and the UK GDPR. These laws ensure that organisations take proper security measures to protect sensitive data and maintain secure systems. Failure to comply can lead to fines, penalties, and other legal consequences.

CAF

The Cyber Assessment Framework (CAF) is a set of guidelines from the UK's National Cyber Security Centre designed to help organisations strengthen their cyber resilience. Created for essential services and those subject to the NIS Regulations, its flexible approach makes it useful for any organisation looking to improve cybersecurity. The framework applies to both IT and Operational Technology (OT) systems and is built around 14 key security principles, supported by detailed Indicators of Good Practice (IGPs). It focuses on four main objectives: managing security risks, protecting against attacks, detecting threats, and minimising the impact of incidents. Assessments can be done internally or by external regulators, making the CAF a valuable tool for improving cybersecurity and supporting regulatory compliance.

ISO 27001

ISO 27001 is an international framework that helps organisations manage information security by identifying and addressing security risks. Its purpose is to protect information systematically and cost-effectively, ensuring confidentiality, integrity, and availability while promoting a comprehensive approach to security and helping with regulatory compliance. Key principles include protecting sensitive information (confidentiality), ensuring data accuracy (integrity), and making sure information is accessible when needed (availability). ISO 27001 provides an Information Security Management System (ISMS) framework. To implement ISO 27001, organisations conduct risk assessments, apply risk treatment strategies, implement security controls, develop relevant policies, and carry out internal audits to assess compliance. Achieving certification shows a commitment to information security and helps improve operational performance and cyber resilience.

GDPR

The General Data Protection Regulation (GDPR) is a law that protects personal data in the UK and European Union, which came into effect in 2018. It gives individuals more control over their data, ensures that businesses and citizens have the same rights across the EU, and safeguards personal data from unauthorised access. It also provides greater transparency about how personal data is used. The GDPR applies to all organisations in the EU, those offering goods or services to the EU, and businesses that monitor EU citizens, including small businesses that handle customer data. The key principles of the GDPR include lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. Data subjects have several rights under the GDPR, such as the right to access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, and the right to object.

NIS

The NIS Directive is an EU cybersecurity law designed to protect critical services from cyberattacks and other threats. After Brexit, NIS is still applicable in the UK. It applies to operators of essential services and relevant digital service providers. The directive ensures a common level of security for network and information systems, requiring organisations to take both technical and organisational measures to manage risks and report significant security incidents. It applies to essential services like gas and electricity companies, as well as digital service providers such as online marketplaces, cloud services, and search engines. The Information Commissioner's Office (ICO) enforces the directive, with powers to issue fines, and can take action against EU member states that fail to comply.

CYBER ESSENTIALS

Cyber Essentials is a government-backed certification scheme designed to help organisations set up basic cybersecurity measures. It is a compliance framework and not a regulation and focuses on protecting against common cyber threats and is a great starting point for businesses of all sizes. The scheme covers key areas like firewalls, software updates, malware protection, access control, and secure system settings. The National Cyber Security Centre (NCSC) recommends Cyber Essentials as a minimum security standard for all organisations and provides guidance, advice, and resources to help improve cybersecurity. Simon Newman, a Director of Cyber London, says:

"Cyber Essentials is the government's standard accreditation scheme for cyber. The benefit for me is that it's demonstrating to customers, staff and suppliers that you have achieved a level of compliance against a recognized government scheme around cyber. It shows that you take data and cyber seriously, which is really good, not just your own data but your customers' data as well."

Cyber Essentials Plus

There are two levels of Cyber Essentials certification. The basic level, known as Cyber Essentials, requires a business to complete a self-assessment and pay a fee to the IASME certifying board. The more advanced Cyber Essentials Plus certification includes the same security measures but, instead of a self-assessment, involves an independent assessor conducting a technical audit of systems, end-user devices, internet gateways, and any services exposed to unauthenticated users online. Enterprise-sized and larger companies should try to obtain ISO 27001 rather than Cyber Essentials, which is a minimum requirement and not sufficient for regulatory compliance. Cyber Essentials was designed to help organisations protect against a range of basic cyber threats but not necessarily all advanced or targeted cyberattacks.

Cyber Essentials Compliance

Any organisation that works closely with UK government institutions or handles sensitive information is required to be Cyber Essentials compliant. Cyber Essentials is a good fit for any organisation, regardless of size or sector, whether based in the UK or elsewhere. Businesses that deal with highly sensitive data, where a breach could cause serious harm, are strongly advised to get certified. Failing to comply can lead to hefty fines, lost business, and serious damage to a company's reputation.

Cyber Essentials Challenges

Complying with Cyber Essentials can be challenging for many organisations due to the time, resources, and effort required. Here are some key challenges businesses may face:

- **Time-Consuming** - Achieving compliance takes a lot of time, as organisations must implement all necessary security controls. With frequent updates to Cyber Essentials guidelines, keeping up can feel like a never-ending task.
- **Lack of IT Resources** - Many organisations struggle with limited IT resources, making it difficult to scan systems for security issues and fix them in line with Cyber Essentials requirements.
- **Frequent Audits** - Regular security audits add to the workload, requiring businesses to constantly review, apply new security measures, and prepare reports for upcoming assessments.
- **Different IT Environments** - Modern businesses operate in complex IT environments, and each system may have specific compliance rules. Manually checking and fixing security issues across multiple systems can be a daunting task.

In his Amazon bestseller, You Don't Need a £1 Million Cybersecurity Budget, Izak asked Simon what the obstacles to getting Cyber Essentials are. Simon said:

"One thing is the cost. Something that appears to be £300 or £400 becomes £2,000 or £3,000 very quickly. Secondly, it's the access to that expertise to help people get to that point and do the things that need to be done. The other challenge for me is that Cyber Essentials is kind of a one-size-fits-all approach, and that may be one of the reasons why there's been such a low uptake. I think that most people who take Cyber Essentials do it because they're required to do so, as opposed to seeing the value in it, which I think is a cause for concern."

Non compliance

In the UK, penalties for cybersecurity non-compliance can include fines of up to £17.5 million or 4% of global turnover, whichever is higher, for breaches of data protection laws like GDPR and the Data Protection Act 2018, as well as potential imprisonment for cybercrime under the Computer Misuse Act 1990. Non-compliance can also result in the loss of certifications such as ISO 27001. Also worth remembering is that fines imposed by regulatory bodies do not include any legal action by third parties. For example, you can get sued by clients or suppliers.

Making a start

Starting a cybersecurity compliance programme might seem overwhelming, but breaking it down into manageable steps can help.

- **Create a Compliance Team** - The IT team plays a key role in cybersecurity compliance, but all departments should collaborate to maintain good security and help with compliance measures.
- **Set Up a Risk Analysis Process** - Identify key systems, assess risks, analyse the likelihood and impact of threats, and decide how to handle any risks - whether to mitigate, transfer, or accept them.
- **Set Controls to Mitigate Risk** - Implement security controls, such as encryption, firewalls, password policies, employee training, and incident response plans, to protect your organisation from cyber threats.
- **Create Policies** - Document clear policies on how these security controls should be followed, which will be useful for internal and external audits.
- **Monitor and Respond Quickly** - Keep track of any changes in regulations or policies and make sure you can respond swiftly to any potential cyber threats before they escalate.

Compliance Consultancy

Cybersecurity consultancy involves offering expert advice and services to help organisations protect their systems and networks from cyber threats. Consultants assess security, identify vulnerabilities, and recommend solutions to strengthen defences.

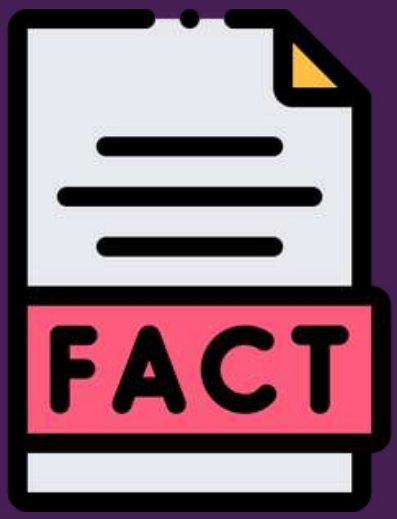
- **Services they offer** - vulnerability assessments, penetration testing, security policy development, security awareness training, incident response planning, and cloud security consulting
- **Why they're valuable** - they bring expert knowledge to organisations lacking internal expertise, offer unbiased security assessments, help avoid costly security breaches and downtime, and ensure compliance with industry regulations
- **Key skills** - technical knowledge of systems and security, analytical ability to spot risks, clear communication with non-technical teams, and problem-solving to create effective security solutions

Benefits of compliance

Having proper cybersecurity compliance in place offers several benefits:

- Protects your reputation
- Maintains customer trust
- Builds confidence and loyalty
- Helps prepare for potential data breaches
- Strengthening overall security

These advantages can directly impact your organisation's success, as reputation, customer loyalty, and trust are key drivers of business growth. Beyond these, staying compliant can also enhance your security and protect valuable intellectual property, such as trade secrets, product specs, and software code, giving you a competitive edge. Compliance is not just about meeting regulatory requirements. It is about building a business that is secure, resilient, and trusted. Compliance should be a core business priority, backed by an appropriate budget, leadership support, and operational integration.



- 44% of companies are using AI to optimize the compliance process
- 68% of financial firms say AI in risk and compliance is a top priority
- 34% of businesses lose prospects because they don't have certification
- 48% of companies spend less than £50,000 annually on audits, while 27% spend between £50,000 and £100,000
- 52% of companies report compliance certification as a top 3 priority for maintaining security

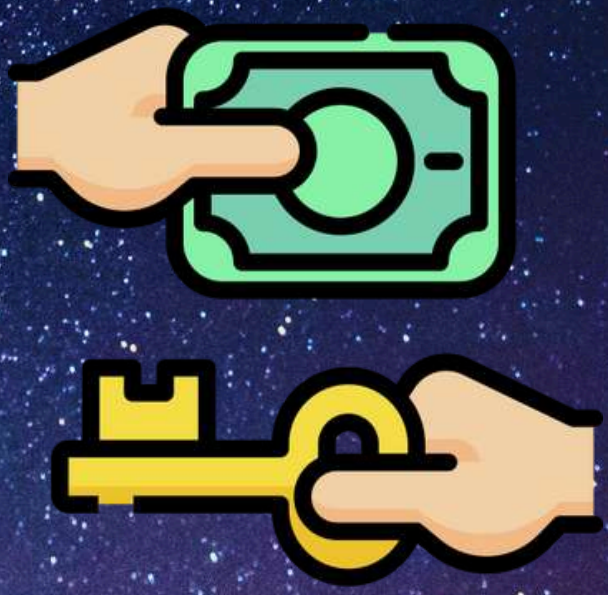
zhero

Compliance insights

Lucindi Storme is our highly qualified and experienced Compliance Consultant. Here, Lucindi tells us why compliance isn't an option but a must-have.

In today's regulatory and threat landscape, compliance is not just a legal requirement—it is the foundation of a secure, resilient, and sustainable business. Compliance is not only about meeting obligations but also about embedding it into the very fabric of business operations. Effective compliance should not be viewed as a burden or an afterthought; it must be a core business function, supported by adequate resources, strategic alignment, and leadership commitment.

Compliance is not optional



Compliance is a business imperative. Every organisation operates within a regulatory framework, whether dictated by GDPR, FCA regulations, NIS 2 Directive, or industry-specific mandates. While these laws set the baseline, compliance is more than just avoiding fines or passing audits—it is about protecting the business, its customers, and its reputation.

zhero

Non compliance consequences

Non-compliance has real consequences:

- Financial penalties – Regulatory bodies impose substantial fines for violations.. GDPR fines can reach €20 million or 4% of global annual turnover.
- Operational disruption – A compliance failure can lead to data breaches, cyberattacks, or service outages, severely impacting business continuity.
- Reputational damage – Trust takes years to build and seconds to lose. Non-compliance erodes customer confidence, investor trust, and market standing.

To mitigate these risks, compliance should not be treated as a checkbox exercise. It must be embedded in business strategy, governance, and daily operations.

Compliance budgeting

Budgeting for compliance is a business investment, not a cost. One of the biggest challenges in compliance is securing adequate funding. Compliance does not generate direct revenue, making it easy for leadership to deprioritise its budget. However, failing to invest in compliance can cost significantly more in the long run. Without a realistic budget, compliance efforts become reactive rather than proactive, increasing risk exposure. Compliance leaders must advocate for compliance as a business enabler, not just a cost centre.

Budget allocation

Key areas where compliance needs dedicated budget allocation:

- Personnel & Training – Skilled compliance professionals, ongoing staff awareness training, and certifications for security teams.
- Technology & Automation – Security and compliance tools, such as SIEM, vulnerability management, and data protection solutions, streamline compliance efforts and reduce risk.
- Third-Party Audits & Advisory – External assessments help validate compliance efforts and identify gaps before regulators or cybercriminals do.
- Incident Response & Crisis Management – A well-funded compliance function ensures rapid response capabilities, reducing downtime and financial impact in case of incidents.

Business integration

For compliance to be truly effective, it must be integrated into business operations, not siloed as an IT or legal function. This requires:

- Executive Buy-In – Compliance must be championed at the board and C-suite level, ensuring leadership commitment and strategic alignment.
- Cross-Department Collaboration – Compliance cannot exist in isolation; it must be embedded in HR, IT, finance, and procurement to cover all operational risks.
- Proactive Risk Management – Compliance should anticipate regulatory changes, cybersecurity threats, and evolving industry standards, rather than reacting after an incident occurs.
- Continuous Improvement – Compliance is not a one-time project; regular audits, policy reviews, and adaptive strategies ensure long-term resilience.

REAL WORLD COMPLIANCE

Strong cybersecurity has never been more important in today's digital world. As organisations deal with ever-changing cyber threats, having solid cyber defences and cybersecurity compliance is essential. Here, we have four real-world case studies exploring how top global organisations protect their digital assets and sensitive data, thereby becoming more compliant – both from a framework and regulatory perspective. These organisations aimed to avoid potential vulnerabilities through proactive threat detection systems, comprehensive risk management protocols, and continually innovating security technologies. By constantly improving security measures, these companies have striven to reduce security risks, keep their systems protected, and significantly improve their cybersecurity compliance. When you examine these cases, you'll gain a clearer understanding of the critical role cybersecurity plays in the contemporary digital arena and the essential measures companies must adopt to secure their digital frontiers.

Enhancing network security

Challenge

Cisco faced challenges in securing its vast network infrastructure against sophisticated cyber threats. Their goal was to strengthen security by predicting breaches before they occurred.

Solution

Cisco developed a predictive analytics tool, Cisco Secure Network Analytics, powered by machine learning to analyse network traffic patterns and detect anomalies that could indicate potential threats. Integrated with existing security protocols, this system enables dynamic defence adjustments and provides real-time alerts to administrators about possible vulnerabilities.

Overall Impact

- **Stronger Security Measures** - The predictive system allowed for a proactive approach to cyber threats, significantly lowering the number of successful attacks. By extension, this meant that Cisco's compliance had definitely gone up a few notches.
- **Greater Efficiency** - Automating threat detection and response streamlined network security management, reducing the need for manual monitoring and resource allocation.

Key Takeaways

- **Proactive Cybersecurity** - Predictive analytics helps organisations identify and mitigate threats before they escalate.
- **The Power of Machine Learning** - Machine learning plays a vital role in spotting patterns and anomalies that human analysts might miss, enhancing overall security.

Strengthening endpoint security

Microsoft

Challenge

Microsoft struggled to secure a vast number of global devices, particularly protecting sensitive data across various platforms vulnerable to advanced cyberattacks.

Solution

To enhance security, Microsoft implemented an advanced encryption system, E2EE, combined with multi-factor authentication, ensuring data remained protected both in storage and during transmission. This solution seamlessly integrated with Microsoft's existing security frameworks, using strong encryption algorithms and adapting in real time to evolving threats.

Overall Impact

- **Stronger Data Security** - Encrypting data across all endpoints significantly reduced the risk of breaches, keeping sensitive information out of reach from unauthorised access.
- **Boosted User Trust** - The improved security measures increased confidence among users, reinforcing Microsoft's reputation and encouraging adoption in high-security environments.
- **Enhanced compliance** - Endpoints are usually the most vulnerable part of any network. When these are made more secure, the vulnerability of the entire infrastructure is reduced and a company is much more compliant.

Key Takeaways

- **The Power of Encryption** - Encryption remains a key tool for protecting data across devices and is a crucial part of any strong cybersecurity strategy.
- **Adaptive Security is Essential** - Flexible, evolving security solutions are vital for staying ahead of constantly shifting cyber threats and preventing vulnerabilities.

Implementing zero trust

Challenge

As remote work expanded, IBM needed to strengthen its data security strategy to protect internal networks from vulnerabilities and ensure that only authorised users and devices could access specific network segments.

Solution

IBM adopted a Zero Trust security model, enforcing strict verification for every access attempt across its network. This approach included strong identity checks, network micro-segmentation, and least privilege access controls, alongside real-time threat detection and response to dynamically enhance security.

Overall Impact

- **Improved Security Compliance** - Implementing Zero Trust architecture enabled IBM to meet strict compliance standards and safeguard sensitive data effectively.
- **Fewer Data Breaches** - By enforcing strict access controls and continuous verification, IBM significantly reduced the risk of data breaches.

Key Takeaways

- **The Importance of Zero Trust** - A Zero Trust approach is essential for organisations aiming to protect critical data in increasingly complex IT environments.
- **Ongoing Verification is Key** - Regular and thorough verification processes are vital to maintaining security integrity in an ever-evolving threat landscape.

Improving phishing defence

Google

Challenge

With its vast ecosystem and large user base, Google was highly vulnerable to sophisticated phishing attacks that traditional security measures struggled to prevent.

Solution

Google introduced a real-time user education programme, Google Safe Browsing and Gmail anti-phishing protection within its email services. This system flags suspicious emails and provides users with contextual information and tips on identifying phishing attempts. Machine learning algorithms continuously refine the system, adapting to new phishing tactics.

Overall Impact

Greater User Awareness - By educating users at the point of potential risk, Google has significantly improved awareness and prevention of phishing attacks.

Fewer Successful Phishing Attacks - The proactive educational approach has led to a marked decrease in successful phishing attempts, strengthening overall user security.

Improved compliance: Google markedly improved its security, making the company less open to fines, penalties and lawsuits.

Key Takeaways

- **The Value of User Education** - Ongoing user education is essential in combating phishing and other social engineering threats.
- **Adaptive Security Systems** - Leveraging adaptive learning systems that evolve with changing attack methods is crucial for effective cybersecurity.

Meet the team

Courtney October

SERVICE DESK ENGINEER

Hi Courtney! What made you realise you want to go into the IT industry?

Watching my dad work with vintage tech, taking things apart, investigating, and fixing them really inspired me. I hope one day I can be as skilled an engineer as he was.

What's your most-used productivity tool?

Hands down, it would be ChatGPT! It's an incredible tool that helps me brainstorm, research, and organize ideas quickly.

How would you describe yourself?

II find joy in solving problems and collaborating with others to achieve great results. My curiosity and passion for discovery drive me every day!

What do you enjoy the most about your role?

If I could, I'd spend all 24 hours a day learning and improving to tackle the daily tasks and challenges even better. I'm excited to see how much I can grow and fine-tune my skills in this field.

Do you have any hidden talents or hobbies?

I'm really passionate about reading and hiking. Anything that brings me closer to nature and allows me to take a moment to breathe and appreciate the scenery is always a win in my book.

What is your favourite movie or TV show?

The Office! I've probably binge-watched and re-watched it more times than I can count. My favourite characters? It's a tough call, but I'd have to say it's a tie between Michael and Dwight.

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos