WHY COMPLIANCE DOES NOT EQUAL CYBER SECURITY

//BAD_ RABBIT>

Q:

WHY ISN'T TICKING THE BOX FOR COMPLIANCE EQUAL TO REAL CYBER SECURITY?

A:

Sometimes business executives assume that being "compliant" with certificate authority is the same as being "secure."

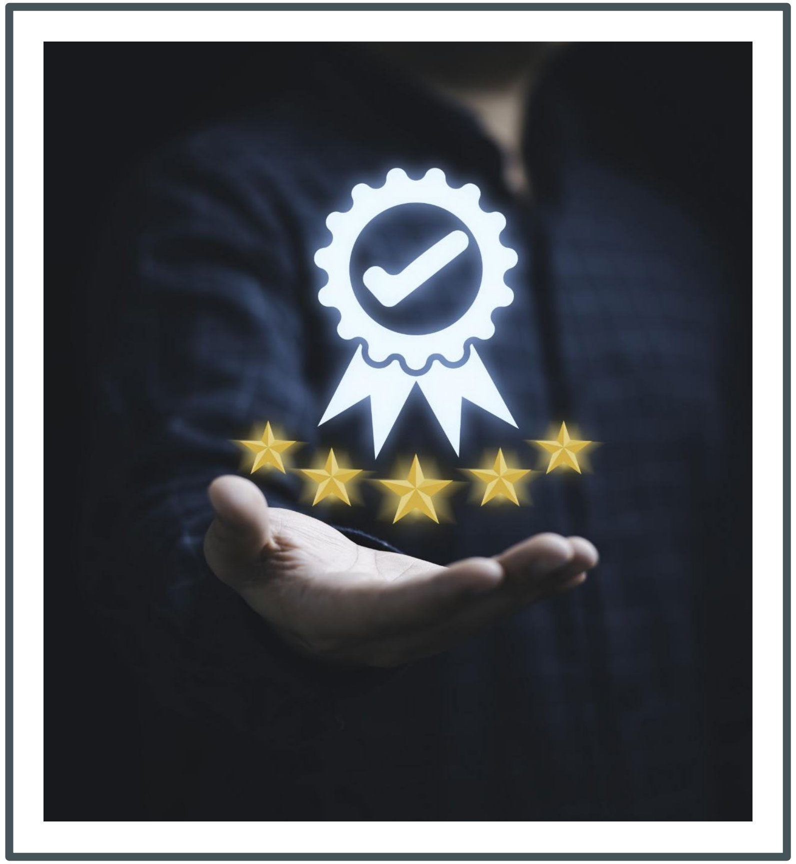
It's not...although both Compliance and Security are vitally important to your business.

Many Bad Rabbit Security clients, from our smaller startups and SMEs through to larger regulated entities, are required to demonstrate their cyber and information security for a variety of reasons, be it to secure larger contracts and pass due diligence, or to meet licensing conditions for regulators, or to meet national and international legal requirements.

Often the most efficient way to demonstrate this is to obtain third-party certification or audit, against recognised security standards such as SOC2 and ISO 27001/2, and to provide objective third-party evidence of achievement. But this is compliance - not security against DDoS, data breaches, viruses, hackers, worms, cybercrime, etc.

Q:

WHILE WE’RE ON THAT SUBJECT, HOW DOES CERTIFICATION HELP BUSINESS?



A:

Audit and attestation to internationally recognised frameworks and standards such as SOC2, ISO27001/2 and Cyber Essentials, are really valuable in demonstrating a basic commitment to cyber security and can be very useful in helping to sell services or products to your new customers.

They provide third party assurance that your company's systems and processes are reliable, have availability, integrity and confidentiality, and protect the privacy of data.

The problem is that the sheer scale of the time, cost and resources required to comply can often be overwhelming. Whether you are a small or large business, all your frameworks require specific controls to be implemented, tested, and documented by detailed evidence.

Q:

SO HOW IMPORTANT IS COMPLIANCE IN BUSINESS?

A:

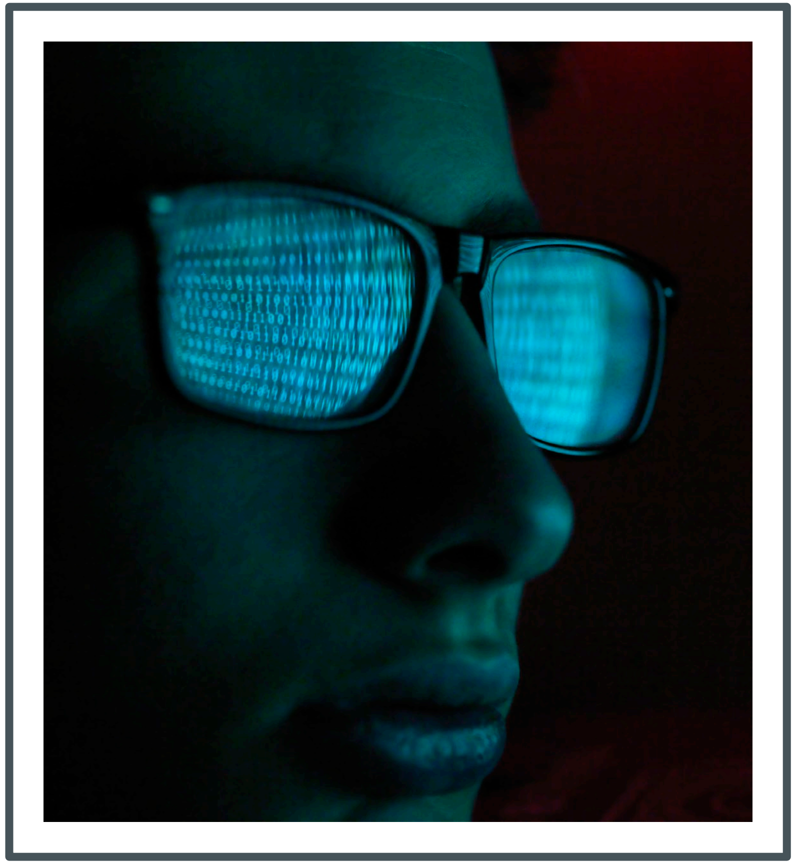
Compliance is important - with or without certification. Any mature cyber security program needs a suitable compliance program. This is to enable you to monitor and assure your security controls are operating as intended and being objectively measured.

Evidence of compliance must be regularly reviewed as part of good governance - even if there are no external auditors involved – so that continuous improvement can be made.

However, whilst achieving compliance is both important and beneficial (and in some cases even required to do business with certain companies) it is *not the same* as being *secure* – certifications and audits alone will not mitigate the risk of a cyber attack or serious incident.

Q:

COMPLIANCE IS GOOD BUT WON’T STOP THE HACKERS?



A:

We see so many examples of companies being breached even if they maintain regulatory compliance to the letter of the law.

The point is that compliance programs will not secure your business if you do not understand where your risk lies. Even though they apply to your frameworks, they often only apply to a subset of your company’s systems or business units.

What Bad Rabbit Security does is to undertake in-depth, full-threat risk assessments covering cyber risk, regulatory risk, and resilience risk such as business continuity, adverse weather, disaster recover and ransomware.

It’s also important to conduct gap analysis on your current controls, processes, policies and procedures to give you a clear and full picture of what you need to do to be secure and resilient. We do all of this as part of our vCISO and Risk services.

Q:

CAN YOU GIVE US SOME OF THE TECHNICAL DETAILS OF RISK MITIGATION?

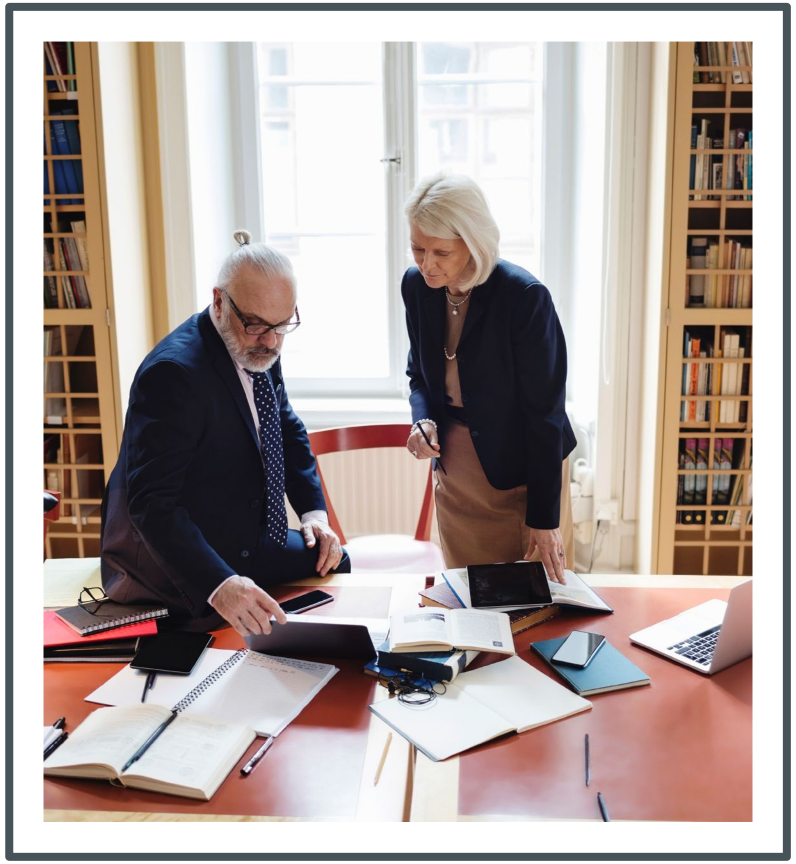
A:

We can map all of this to any of the common frameworks and standards such as SOC2, ISO27001/2, CIS, NIST CSF and others. We then guide you in the selection and deployment of cost-effective right-sized technical controls, such as next-gen firewalls, SIEM and SOAR. We even deliver managed security services (MSSP) such as EDR/XDR, and a 365/24/7 Security Operations Center.

We also conduct penetration testing and vulnerability scanning, this lets you understand your exposure and threat surface. Then we provide full guidance on remediation and control implementation to address vulnerabilities. This is to give you both compliance requirements, and to enable you to remediate real-world security issues and mitigate your risk.

Q:

HOW DO COMPLIANCE AND CYBER SECURITY WORK TOGETHER TO PROTECT COMPANIES AND THEIR DATA?



A:

While compliance mandates basic security standards for companies, cybersecurity takes a proactive approach to safeguarding a company’s technology.

Compliance is important because failure to follow standards set by regulators can result in financial or legal penalties and reputational damage. However, cybersecurity is equally, if not more vital, because of the increasing number of cyber threats that companies face on a daily basis.

Being compliant is important to give customers the confidence that your company protects their data, but only by developing your actual security program to understand your risk, will you be truly secure – and then getting compliant is a whole lot easier!

CONTACT US

You can read more about compliance, risk and cyber services on Bad Rabbit Security website and contact us on any issues raised at

info@badrabbitsecurity.com

Learn more about our services

Visit the Bad Rabbit Security website