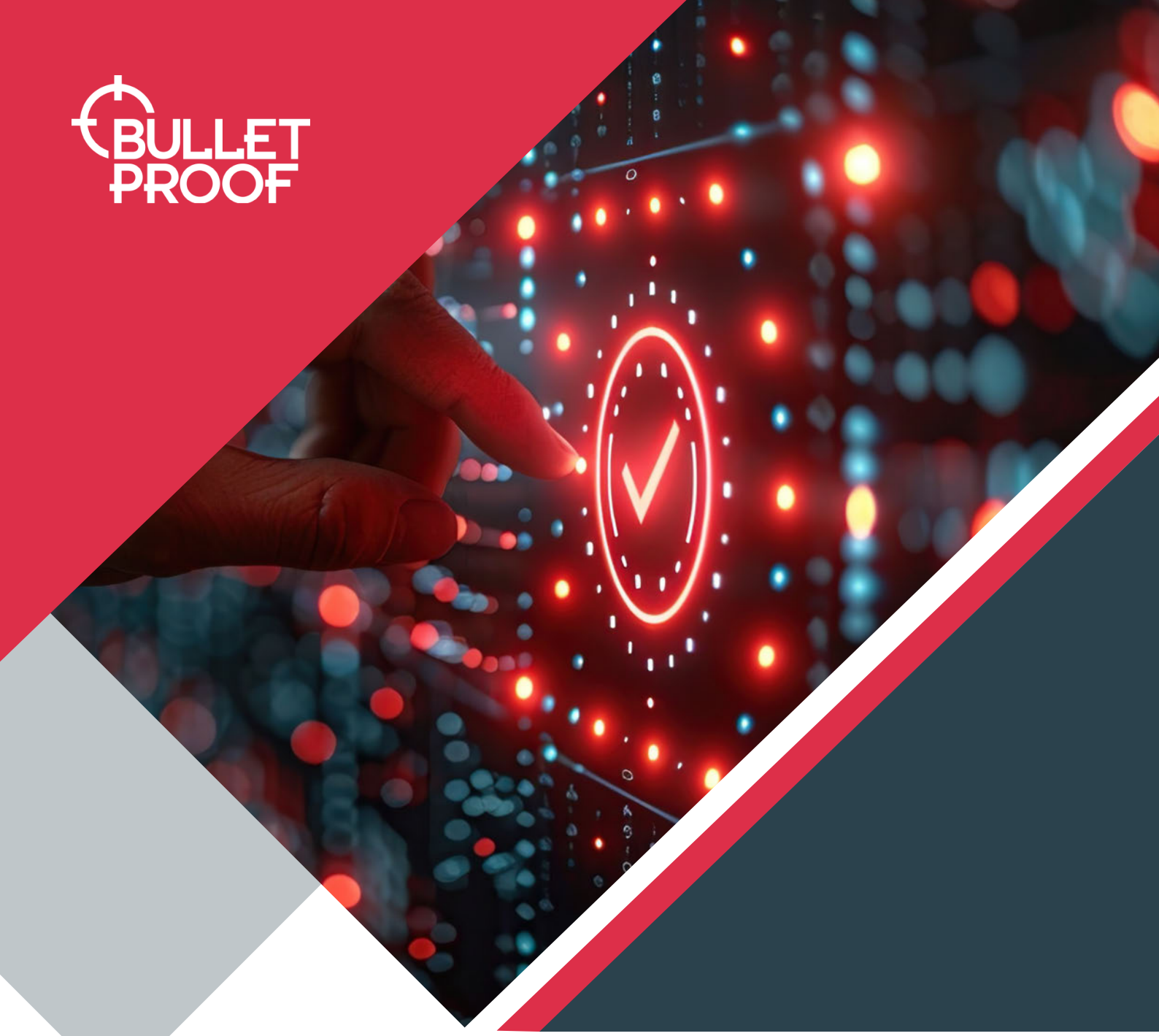
BULLET PROOF



10 POINT SECURITY CHECKLIST

Boost your security defences with this 10-point security assessment checklist

www.bulletproof.co.uk

"With a third of UK businesses identifying cyber attacks[1] and supply chain security on every board's agenda, cyber securtiy is a key priority for businesses in all industries. That's why Bulletproof has put together this 10-point security checklist. It's designed to help your organisation make sure it's doing all the right things to stay secure.

Nicky Whiting
Managing Director

1 SECURITY SCANNING

Research has shown that cyber criminals can detect online devices within 0.3 seconds[2]. This makes knowing what your easy-to-exploit vulnerabilities are an essential first step to protecting your business. Thankfully getting visibility of your top-level attack surface and system vulnerabilities is easy and straight forward with automated VA scans – you just have to make sure you're doing it.

- ☐ Run periodic attack surface scans to see what intel is freely available to potential hackers
- ☐ Schedule monthly or weekly vulnerability scans (VA scans) to keep on top of newly disclosed threats
- ☐ Customise the scans to suit different infrastructure components & applications
- ☐ Ensure you're using an up-to-date scan engine from a reputable provider
- ☐ Perform additional ad hoc scans on new deployments & new environments
- ☐ Review the scan results & create a prioritised list of activities
- ☐ Track each threat through its remediation cycle

To get started with security in any form, you need to know what your vulnerabilities are. It's the job of a VA scan to tell you this.

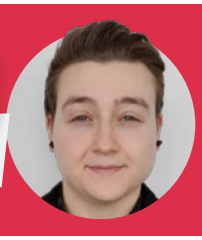
2 PENETRATION TESTING

Penetration testing is the cornerstone of any cyber security strategy, and regular pen testing is recommended or required by many compliance standards. It picks up where security scanning leaves off, using human expertise and ingenuity to find security flaws that an automated scan never could. Key to penetration testing's value is getting the right scope, so make sure your pen test provider will take the time to understand your objectives.

- ☐ Penetration test at least annually
- ☐ Larger organisations should split penetration testing into separate projects for easier management
- ☐ Test all components of your infrastructure, including applications & cloud environments
- ☐ Make sure your provider has recognised industry certifications, such as CREST and OSCP
- ☐ Get a sample report to verify that the test represents good value for money
- ☐ Look for a provider who can provide prioritised results with actionable remediation advice
- ☐ The best providers has a portal-based results delivery to help you track & manage your threats

Without a penetration test, the first time you'll find out about an exploitable security weakness is when you're hacked.

PRO TIP



"A good penetration test provider will include a year of vulnerability scanning and attack surface scanning as part of the package.

Jordan Constantine
Penetration Testing Manager

3 CYBER ESSENTIALS

Cyber Essentials is a great security foundation, with 93% of UK businesses confirming that Cyber Essentials certification protects them against common cyber threats[3]. Cyber Essentials is UK Government backed and refreshed regularly to keep it a relevant, valuable certification. Both Cyber Essentials and Cyber Essentials Plus are required for bidding on public sector contracts, meaning it's applicable to everyone from startups to multi-national enterprises.

- ☐ Assess if Cyber Essentials or Cyber Essentials Plus is the right level of certification
- ☐ Consider a consultant-led Cyber Essentials package that makes it easier to meet compliance
- ☐ Make sure your provider is registered with Cyber Essentials & can demonstrate a proven track record of passing customers
- ☐ Look for partners who are registered Cyber Advisors
- ☐ Download the questionnaire in advance to anticipate any non-compliant areas

Cyber Essentials Plus is an enhanced certification that allows you to win more contracts and demonstrates a better standard of security.

4 CYBER SECURITY ASSESSMENT

A Cyber Security Assessment, or health check, is a comprehensive review of the information security and cyber security measures in place across your business. This helps you understand your current security posture, find weaknesses and opportunities, and create a roadmap to improve your security. They're an ideal starting point for businesses looking to mature and evolve their security posture. As an independent evaluation, they can validate your existing controls & highlight bias and assumptions.

- ☐ Look for security assessments that align to ISO 27001 or NIST 800-53 standards
- ☐ Allocate internal resources to support the assessment
- ☐ Ensure that outsourced providers (e.g. IT service providers) are in scope of the assessment
- ☐ Ask for a sample report to ensure it's easy to understand, with clear & unambiguous red/amber green ratings
- ☐ Consider a security assessment that differentiates areas in need of immediate attention from longer-term opportunities
- ☐ Make sure your provider has experience in information security with certifications & experience to back up any claims

---

The Bulletproof Cyber Security Assessment can be used to demonstrate your cyber security maturity to customers, your supply chain and stakeholders.

5 SECURITY TRAINING

Billions of phishing attacks sent every day, and up to 79% of all cyber attacks include phishing[4]. So it's no surprise that security training has become essential component of any security assessment checklist. Your staff represent your biggest attack surface, so your business needs to ensure that all staff are aware of their security responsibilities. Building these best practices into your day-to-day staff operations can dramatically reduce your risk of breaches.

- ☐ Assess if on-site or virtual training is the right option for your needs
- ☐ Consider combined training that covers security & data protection
- ☐ Build training into staff on-boarding
- ☐ Conduct at least annual security awareness training
- ☐ Find a provider who makes securtiy entertaining & novel to boost engagement
- ☐ Test knowledge retention with tests
- ☐ Ensure learning is embedded through the business

Bulletproof security training has the potential to be one of the most powerful tools in your cyber defence arsenal.

PRO TIP

"A good cyber security assessment can be used as a business case to secure future security funding & investment.

Luke Peach
Head of Compliance Services

6 RISK MANAGEMENT

The next step is to codify your security activities in a formal risk management framework, such as ISO 27001. Taking a risk-based approach to managing information security means you can provide assurance that your people, processes and technology are working together maintain an appropriate level of security. For this reason, ISO 27001 is often contract requirements as part of supply chain security and supplier due diligence.

- ☐ Assess which risk management framework is right for you, such as ISO 27001, SOC 2, or NIST 800-53
- ☐ Allocate the right internal resources & get management buy-in to ensure the project is supported
- ☐ Consider using a consultant-based service over downloadable toolkits to expediate the project
- ☐ Look for a provider that has experience with multiple industries so they can bring problem solving knowledge to your implementation
- ☐ Ensure on-going maintenance of risk management is embedded ahead of the project completion

Effectively managing your risks lets you allocate resources effectively. This means you maximise security impact without overspending.

7 DATA PROTECTION MANAGEMENT

A core principle of data protection is ensuring data is stored, processed and transferred securely. This puts data protection management firmly in scope of any security posture assessment. A lot of businesses tell us managing data protection in-house is a significant challenge, which is why outsourced support is so popular.

- ☐ Talk to your data protection officer to find evidence of data security management
- ☐ Ensure IT teams are following data security procedures
- ☐ Consider leveraging data privacy standards, such as ISO 27701
- ☐ Ensure all data protection activities have senior management buy-in
- ☐ Make sure your data protection officer is in regular contact with your vCISO to find synergies and savings

Outsourcing data protection management makes it easy for your business to focus on the day-to-day.

8 VIRTUAL CISO

Making sure everything on this security checklist is working together requires expertise and experience. But with 77% of in-house CISOs citing stress as impacting their physical health[5], hiring and retaining a CISO is both hard and expensive. Virtual CISOs solve these problems by offering the oversight and management you need on a cost-effective retainer basis.

- ☐ Look for a provider with experience in other information security fields
- ☐ Check that the list of vCISO activities meets your operational objectives
- ☐ Don't be afraid to ask for a customised package that gives you exactly what you need
- ☐ Verify that the provider can grow with your business without discontinuity of service
- ☐ Find a vCISO that can work with your DPO to deliver cost savings

---

A good virtual CISO will make sure everything is working together as it should, as well as challenging your information security assumptions and biases.

PRO TIP

"Don't let security compromise productivity. A vCISO can take a big-picture approach and ensure you're effectively managing risk without stifling productivity.

Eze Adighibe
Information Security Manager

9 LOG MONITORING & SIEM

Next it's time to get proactive. Your risk management activity in point 6 of this checklist should have told you when and where to apply either log monitoring, or SIEM, or both. If you're unsure, log monitoring is a good place to start, growing to a managed SOC & SIEM service. This gives you a real-time defence, stopping attacks in their tracks.

- ☐ Assess if log monitoring or SIEM is right for your risk profile & if 24/7 cover is appropriate
- ☐ Make sure log monitoring & SIEM meets your compliance & regulatory requirements
- ☐ Consider how easy the service is to deploy & if it works with your existing security stack
- ☐ Look for a flexible SaaS SIEM solution to minimise overheads & capital investment
- ☐ Find a managed SOC & SIEM provider who can provide simple pricing & an easily scalable service
- ☐ Ask for a demo & ensure there's a clear path to value
- ☐ Ensure you're set up to effectively respond to actions & escalations

---

Find a provider that gives step-by-step remediation advice for each and every security so you can fix issues fast and get back to other tasks.

10 RED TEAMING

Red teaming is an adversarial type of security testing that aims to breach your defences by employing genuine tactics, techniques and procedures that a real-world cyber criminal would use. This goal-based approach gives valuable insights on where hidden threats exist. If you're not sure about what you want from a red team, a good provider will put the work in up-front to help you define clear goals and objectives.

- ☐ Assess which engagement is right: assumed breach, red team, purple team or a blended approach
- ☐ Look for a provider with a track record of red teaming and appropriate certifications (e.g. CREST)
- ☐ Check that their adversarial capabilities are a good fit for your security operations

---

Red teaming uncovers blind spots caused by bias and assumptions, making it great way to test and improve your incident response capability.

LOOKING FOR HELP TAKING THE NEXT STEP IN YOUR SECURITY?

Bulletproof's consultant-led assessment examines your current security posture, finds opportunities, and creates a roadmap to improve your defences and justify security investment.

www.bulletproof.co.uk/cyber-security-assessment

Trusted cyber security & compliance services from a certified provider

CREST. PEN TEST ISO 27001 ISO 9001

HM Government G-Cloud Supplier | Crown Commercial Service Supplier | CYBER ESSENTIALS | CYBER ESSENTIALS PLUS

SOURCES

1, 4 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

2 https://www.bulletproof.co.uk/webinars/5-things-a-hacker-doesnt-want-you-to-know

3 https://www.ncsc.gov.uk/information/setting-baseline-ce-prior-to-iasme

5 https://thehackernews.com/2023/03/cisos-are-stressed-out-and-its-putting.html#:~:text=Work%20fatigue%20has%20caused%2064,grow%20at%20an%20alarming%20rate.

ABOUT BULLETPROOF

We are your best defence against cyber threats. We are Bulletproof.

At Bulletproof, security is in our DNA. We're laser-focussed on bringing innovation and simplicity to all areas of cyber security, information security, and data protection. As an established leader in the UK market, we have the expertise and experience to help you through your challenges

Organisations in all industries trust us to remove the complexities of managing projects in-house, helping SMEs grow and empowering enterprises to work smarter. Combining our years of industry experience with a perfected suite of services, Bulletproof works as an extension of your team to give you full visibility over your threat landscape and proactively manage your risk.

Cyber Security | Information Security | Data Protection

+44 (0)1438 500 500 **contact@bulletproof.co.uk** **www.bulletproof.co.uk**

BULLETPROOF