Consensus Audit Guidelines
Top 20 Critical Security Controls

CRITICAL QUESTIONS YOUR SECURITY PROGRAMS MUST ANSWER

tripwire®

IS YOUR ORGANIZATION'S CYBERSECURITY STRATEGY **SIMPLE AND EFFECTIVE?**

Just because you're paranoid doesn't mean they're not out to get you. Let's face it, businesses just like yours face a multitude of security threats every single day. Many they fend off. Sadly, some they don't.

The secret is to be prepared. But with so many threats from so many sources, how can you be confident you've done everything within reason you can to keep your business safe? Fortunately, help is at hand. Working with the NSA, SANS and the Council on CyberSecurity have identified and ranked the top 20 critical controls every business should have in place. The question is: **Are you ready?**

Check out the questions your security programs must address and find the gaps before the cyber criminals do it for you. Then go deeper with our range of guides and resources to make sure your organization is protected.

Q.1

NSA Rank = Very High

Have you inventoried all your authorized and unauthorized devices?

Yes? Excellent. Go to Question 2.

No? An accurate inventory is a critical foundation in reducing the ability of attackers to find and exploit unprotected systems. If you haven't taken this step, make sure to review our briefing at tripwire.com/control-1

Q.2

NSA Rank = Very High

Have you inventoried all your authorized and unauthorized software?

Yes? Good work. Go to Question 3.

No? While hardware and devices are key, it's vulnerable or malicious software that all too often leaves your organization open to attackers. Minimize or root out attacks by reading our briefing at tripwire.com/control-2

Q.3

NSA Rank = Very High

Have you created a standard hardened image with secure configurations on all your hardware, software and mobile devices?

Yes? Great. Go to Question 4.

No? One of the easiest ways for an attacker to penetrate your defenses is by exploiting services and settings that allow easy access through networks and browsers. Learn to slam the door by checking out our briefing at tripwire.com/control-3

Q.4

NSA Rank = Very High

Do you practice continuous vulnerability assessments and remediation to minimise opportunity for attackers?

Yes? Done. Go to Question 5.

No? Things change. Threats evolve. Just because you're safe right now doesn't mean you won't face a successful attack a week or month from now. Learn how to proactively identify and repair software vulnerabilities with our briefing at tripwire.com/control-4

Q.5

NSA Rank = High / Medium

Are your malware defenses up to scratch?

Yes? Good. Go to Question 6.

No? The threat landscape is continuously evolving as new malicious code is developed and spread to capture sensitive data and damage equipment. If your protection isn't able to counter these ever-mutating dangers, you should read our briefing at tripwire.com/control-5

Q.6

NSA Rank = High

Are you confident your application software is secure?

Yes? Nice work. Go to Question 7.

No? Too much web-based and other application software, whether home-grown or third-party, offers potential attackers easy targets through security flaws or coding errors. If you're not sure that your software is safe, take a look at our briefing at tripwire.com/control-6

Q.7

NSA Rank = High

Have you adequately protected your wireless security perimeter?

Yes? Great, that's one more area safeguarded. Go to Question 8.

No? With the explosion in wireless devices and the necessary access points has come a rapid increase in potential threats. Make sure you're only allowing authorized access matching a security profile and defined business need by reading our briefing at tripwire.com/control-7

Q.8

NSA Rank = Medium

Are you able to recover data quickly?

Yes? Good (there's no time to lose). Go to Question 9.

No? While you will want to do everything you can to protect your organization against an attack, should the worst happen, you'll need to be able to get back up and running fast to minimize the damage. If your data recovery capability isn't as robust as it needs to be, you should read our briefing at tripwire.com/control-8

Q.9

NSA Rank = Medium

Have you carried out security skills assessments and training on your staff?

Yes? Excellent. Go to Question 10.

No? With security threats evolving so fast, it's critical your people stay at the top of their game. This means identifying knowledge gaps and closing them with the right training. To learn more about improving your security practices, take a look at our briefing at tripwire.com/control-9

Q.10

NSA Rank = High / Medium

Have you established secure configurations across your network devices?

Yes? Fantastic. Go to Question 11.

No? The internet is a popular vector for would-be attackers, so it's important you lock down your firewalls, routers and switches. If you need more advice on how to make this happen, check out our briefing at tripwire.com/control-10

Q.11

NSA Rank = High / Medium

Have you restricted access to network ports, protocols, and services?

Yes? Wise move. Go to Question 12.

No? While many businesses need to give employees remote access to a range of services, failing to maintain tight control can offer a direct on-ramp to attack. If you haven't locked down remote access, read our briefing at tripwire.com/control-11

Q.12

NSA Rank = High / Medium

Do you sufficiently control who has admin privileges?

Yes? Good work. Go to Question 13.

No? Admin privileges offer a degree of access any attacker would kill for. If you haven't protected and validated these accounts across all devices, you need to review our briefing at tripwire.com/control-12

Q.13

NSA Rank = High / Medium

Are you sure your network boundaries are protected?

Yes? Great. Go to Question 14.

No? Attackers will often look to access your network from the edges (eg via a compromised machine). To find out how to control the flow of traffic, monitor content and find evidence of attacks, take a look at our briefing at tripwire.com/control-13

Q.14

NSA Rank = Medium

Are you keeping a close enough eye on your audit logs?

Yes? That'll put you in the picture. Go to Question 15.

No? Your audit logs can help you identify attacks—including the location, malicious software deployed and activity on victim machines. If you're not actively monitoring and analyzing your logs, you should read our briefing at tripwire.com/control-14

Q.15

NSA Rank = Medium

Are you working on a need-to-know basis?

Yes? Excellent. Go to Question 16.

No? You will have a range of sensitive data that attackers would love to access. If you're not controlling this on a strictly need-to-know basis, you need to take a look at our briefing at tripwire.com/control-15

Q.16

NSA Rank = Medium

Are you on the lookout for impostors?

Yes? You can't be too careful. Go to Question 17.

No? You need to actively monitor and control user accounts to prevent attackers from impersonating legitimate users and gaining access. If you're currently falling short on this, read our briefing at tripwire.com/control-16

Q.17

NSA Rank = Medium / Low

Can you prevent the loss of sensitive data through network attacks and theft?

Yes? Good. Go to Question 18.

No? To avoid sensitive data from being transmitted (or simply walking out the building), you need to closely scrutinize people, processes and systems. If your data loss prevention isn't up to the task, you should see our briefing at tripwire.com/control-17

Q.18

NSA Rank = Medium

Do you have a fast, effective incident response plan in place?

Yes? Wise move, every minute counts. Go to Question 19.

No? Security controls are not just about protecting data – safeguarding your reputation is vitally important too. If you haven't developed an incident response plan identifying actions, roles and responsibilities, you should check out our briefing at tripwire.com/control-18

Q.19

NSA Rank = Low

Is your network design robust enough to deter attackers?

Yes? Great. Go to Question 20.

No? A robust, secure network design is fundamental to protecting your business. If you haven't put in place a minimum of three layers (DMZ, middleware and private network) you should read our briefing at tripwire.com/control-19

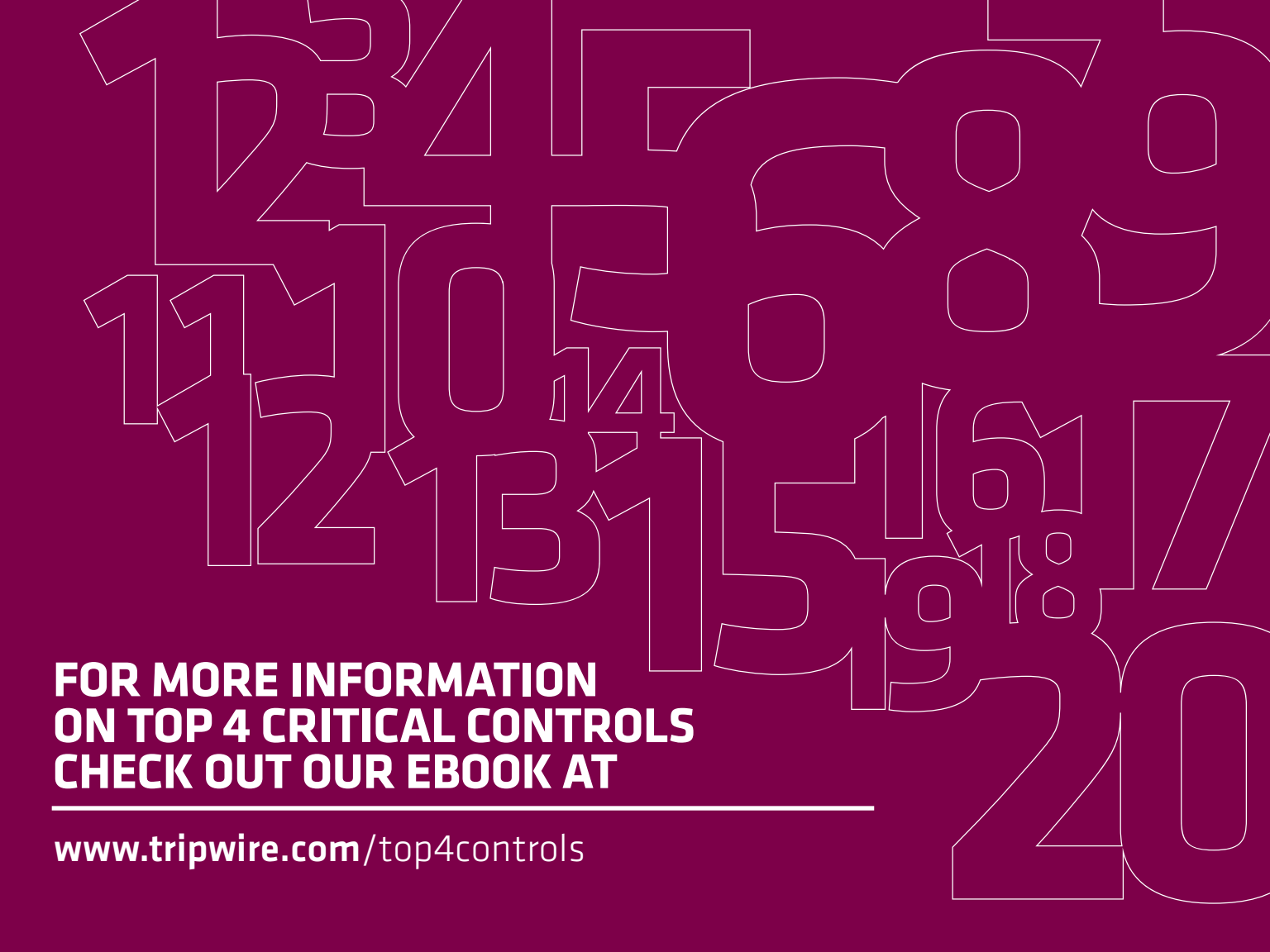
Q.20

NSA Rank = Low

Have you tested your resilience to attack?

Yes? Good work.

No? The time to discover your weak points is not after a successful attack. If you're not running regular internal and external penetration tests, make sure you check out our briefing at tripwire.com/control-20


FOR MORE INFORMATION
ON TOP 4 CRITICAL CONTROLS
CHECK OUT OUR EBOOK AT
www.tripwire.com/top4controls