grant mcgregor
technology · people

Our twelve crucial controls will give you a quick insight into which areas of your business may leave you most vulnerable to a cyberattack - offering access to sensitive company data.

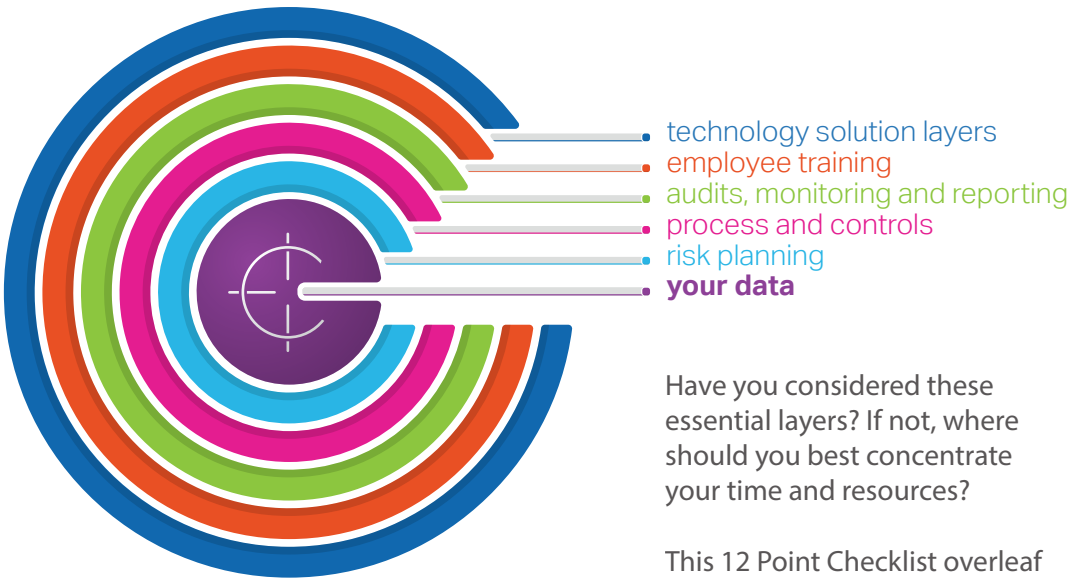
Your data is vulnerable to attack - and there's plenty of evidence that no company is too big or too small to be a target. The personal and corporate data you hold on your systems is worth money to cybercriminals - whilst also being the lifeblood of your business.

Your peers are already taking steps to make sure they're ahead of the threat. What more could you be doing to keep your business competitive and secure?

Cybercrime is fast growing. Can you be sure you are suitably protected?

Cybercrime is not your fault but it is your responsibility to protect both your own and your customers' data.

The 5 Vital Layers Securing Your Data from Cyber Criminals



Have you considered these essential layers? If not, where should you best concentrate your time and resources?

This 12 Point Checklist overleaf will get you started ...

T: 0808 164 4142 **W:** grantmcgregor.co.uk/cyber-security

12 Crucial Controls to Reduce Your Business Risk & Achieve Compliance

Are you on top of managing information & data security risks in your organisation?
Are you compliant with today's standards and protected against evolving threats?

Use this checklist to assess how well you are performing against these common information management compliance standards.

1 IT Assets

Are your IT Assets all securely configured & maintained?

Do you have a comprehensive, up-to-date register of all your IT devices, applications & users? Can you track & manage each asset's security configurations?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

2 Endpoint Protection

Are your devices managed & secured for today's evolving threats?

Is your endpoint protection actively scanning, analysing & quarantining suspicious activity & threats with automated reactions to protect you and your device?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

3 User Access Controls

Do you rigorously control all aspects of User Access?

Do you know who can access what, and to what permission level? Do you audit and control user access rights, passwords, permissions, and Admin accounts regularly?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

4 Security Patches / Updates

Do you apply timely security updates or patches?

Are all installed operating systems & software regularly updated? Do you use a 'critical update' service to protect your computers from the latest known vulnerabilities?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

5 Web Security

Do you employ suitable web content filtering & security?

Do you prevent your people from visiting harmful or unsavoury websites? Is internet gateway security in place to detect & prevent malicious web malware threats?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

6 Incident Response & Recovery

As part of incident response, do you reliable have backup & data recovery?

Nothing is fool proof... Can you readily recover your business data that is accidentally or maliciously deleted or encrypted? From all your systems?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

7 Email Security

Do you have effective email security in place?

Over 90% of attacks originate in email. Do you use a reliable email security gateway that actively scans & protects all emails, web links & attachments? O365 is not enough.

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

8 Multi-Factor Authentication

Have you set up Multi-Factor Authentication?

Passwords are easily compromised. Have you added this layer of protection on top of user passwords to ensure your social media, critical data & systems are better secured?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

9 Next Generation Firewall

Do you employ a next-gen Firewall to screen your network traffic?

Is your firewall effective in preventing, detecting & resolving inbound/outbound network traffic? Is it suitably configured to control access to data & applications?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

10 Security Policies

Do you apply appropriate Data & Information Security Policies?

Are your devices compliant against your Company policies? Should they be able to access your applications & data or are non-compliant devices denied?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

11 User Education & Awareness

Do you promote an incident reporting culture?

How often do your train your people? Do you educate them about data security, threats, policies & best practice? Do you test frequently & monitor the results?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

12 Information Protection

Can you easily locate & retrieve sensitive data when required?

Do you classify your information in terms of confidentiality? Do you have policies & control measures to restrict access & processing rights? Are you GDPR ready?

CE / Plus | CIS | ICO | NCSC | IASME | ISO27001

○ Yes ○ No ○ Don't Know

If you've answered **No** or **Don't Know** to any of the items above then you're at heightened risk of a data breach.

If you've answered **Yes** to all the questions above, you might be ready to get *Cyber Essentials* or beyond.

Ready to defend your organisation and your reputation today?
Then get the certification that will help protect your business...
take your first step at www.grmc.it/completed-checklist