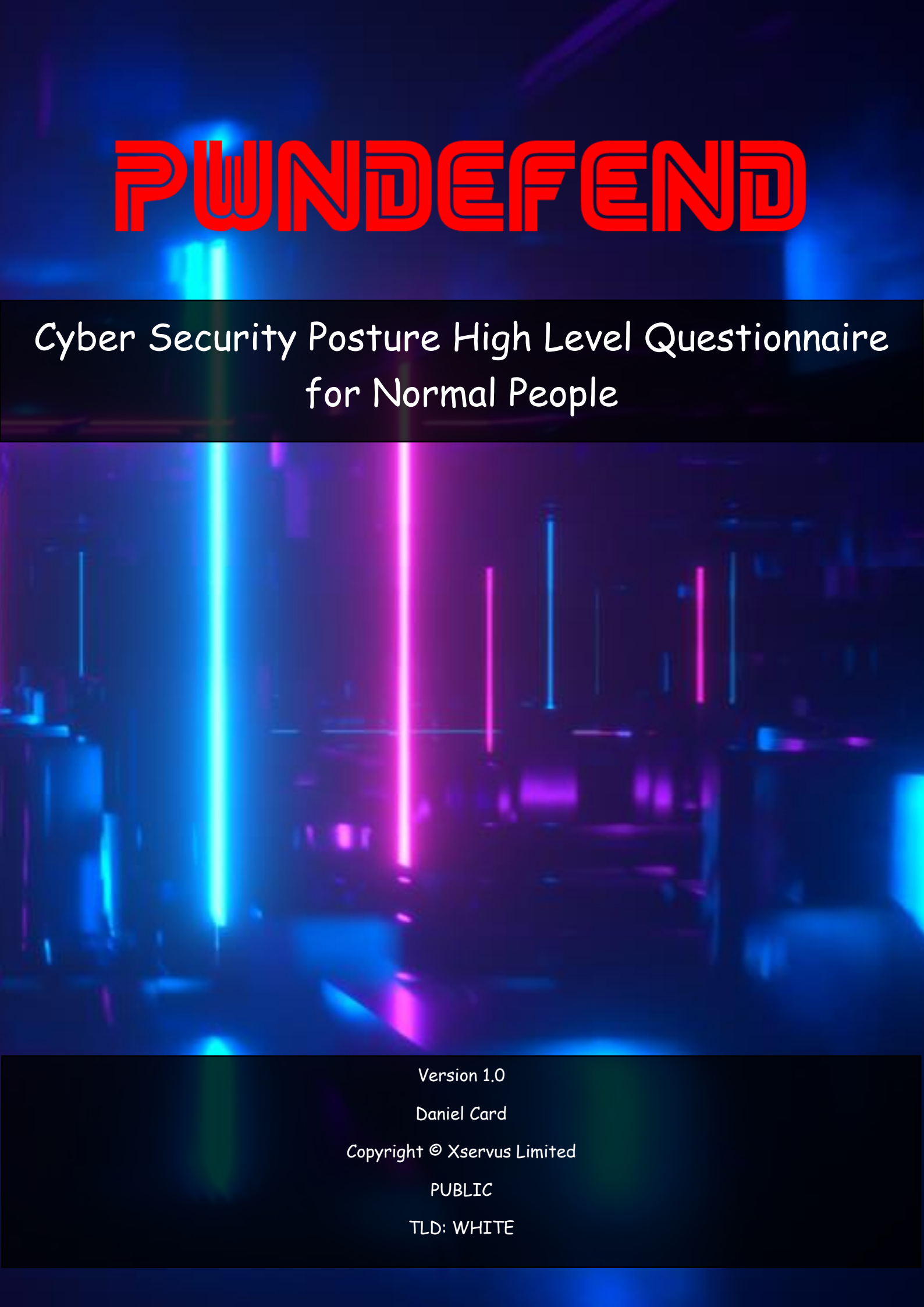


Cyber Security Posture High Level Questionnaire for Normal People

Version 1.0

Daniel Card

PUBLIC

TLD: WHITE

The "do you take your companies cyber security seriously?" questionnaire

Forward

I have worked in the technology and cyber industry for a while, I run across a lot of different scenarios with organisations of all shapes sizes, verticals, maturity levels, revenues, and security postures. I see many of the same patterns across orgs. Security is hard, so I thought I would try and make a small toolkit to help people who are not cyber ninja warriors or information security jedi's to help people get an initial grasp. This toolkit is basic (it is more complex than its initial idea, but it is still mainly just answering yes and no to questions), I have left the original title in as well because I want people to understand the context of why I decided to write and publish this. I even changed the font to comic sans because I want people to realise it is in the vein of the "intro" category and does not cover everything, it is not a glossary of cyber or a how to guide. It is a quick diagnostic tool that should be helpful to most organisations and people regardless of their job title or experience level. It is useful to you that is great, if it's not that's great too (constructive feedback is useful and welcome!). Hopefully, some people find this helps them on their cyber security improvement journey!

- mRr3b00t

Contents

Version Control

Version	Author	Date	Notes	Status
0.1	Daniel Card	09/01/2021	Initial creation	Draft
0.2	Daniel Card	09/01/2021		Draft
0.3	Daniel Card	09/01/2021		Draft
0.4	Daniel Card	09/01/2021	Added CE alignment section	Draft
0.5	Daniel Card	09/01/2021	Added CSF alignment section	Draft
0.6	Daniel Card	09/01/2021	Added more questions in	Draft
0.7	Daniel Card	10/01/2021	Added more questions in	Draft
0.8	Daniel Card	10/01/2021	Added framework and general guidance	Draft
0.81	Daniel Card	10/01/2021	Added minor changes/recommendations from Dirk and added changes from Matt Summers.	Draft
1.0	Daniel Card	01/05/2021	Initial publication to the public	Release

Content Development Team

Lead Author: Daniel Card – TOGAF Certified Architect, ITIL Foundation, PRINCE2 Foundation, Penetest+, MCP, MCSA, eJPT - @UK_Daniel_Card

Technical Reviewer A:

Technical Reviewer B: Anon Cyber Officer

Technical Reviewer C: Dirk Schrader

Technical Reviewer C: Matt Summers

Grammar and Style Reviewer:

Legal Stuff

All frameworks, standards and logos/names etc referenced in this document are property of them etc.

This document was written to help organisations and people understand a bit more about what InfoSec and cyber mean to them and give them an idea of the breadth and depth it covers.

Guidance

Please complete the following questions, if you answer "no" to a few of these then you don't take it seriously!). This is aimed at organisations of sufficient size, scale, revenue or business model that requires formal cyber management. There isn't a one size fits all if you are looking for that you won't find it from me. If you don't understand the question you probably don't take security seriously (get your CISO or CIO/CTO to complete it if you can't). It doesn't matter how you achieve these, you can inhouse, outsource, out resource etc. This is not a detailed review of your security posture, it's architecture or operation model, it's simply a small (yes this is small in our world) list of questions to help you understand if you do indeed take your organisations and your customers security as seriously as you might tell people.

Dan it's over 120 questions, how is that high level? Well when we look at a policy, process and technology etc. from a detailed POV we will be looking at particulars of documentation, particulars of process and capability and will go even deeper. AN example of this is that SOC2 has over 300 points for consideration and the documents that back this stuff up (NIST, ISO etc. are huge) so this really is a light version. You will also find each framework has key points in specific areas. This questionnaire is not meant to replace the other frameworks, more to provide a view across them.

I made this for the community, use it, don't use it, change it, modify it, do whatever just don't try and pass it off as your own please. I gave up a Saturday to write this and to be able to write this from my brain without too much reference architecture and standards checking etc. has taken me a fair few years of learning and experience! I've checked this (ok I haven't yet – I'm going to) against good practises such as:

- NIST
- NCSC CSF
- Vendor Guidance
- ISO27001:2013

And it's (in my opinion) not going against the grain from a general industry frameworks/standards POV. I hope it's useful to people. Given how bad business security postures (and peoples/organisations understanding of cyber) are still in 2021 hopefully this helps at least some people! May the force be with you!

Cyber Security Maturity and Security Posture

Cyber security maturity is a term used to describe the level and depth of experience and skill/practise an organisation has in a range of capabilities. They generally cover areas such as:

- People
- Process
- Technology
- Resources

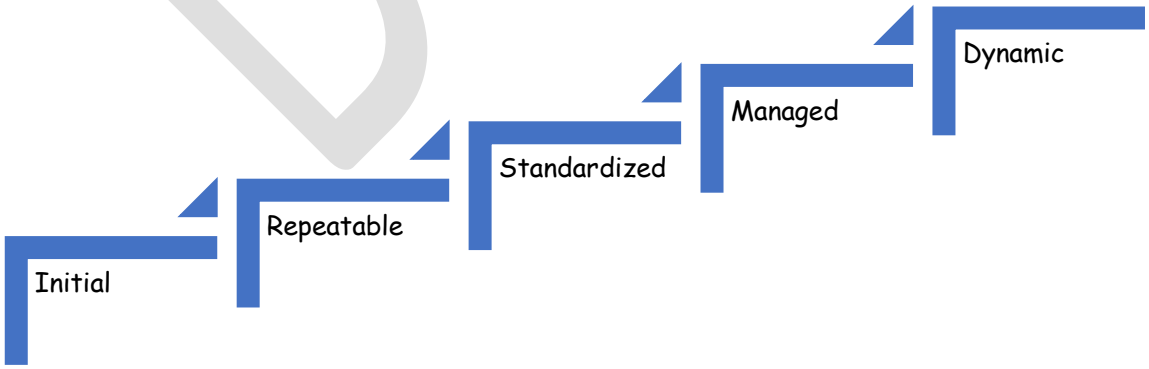
If you are familiar with balanced scorecards, they are similar in that they take a look at an organisation or service from a range of perspectives to combine a range of views into a single view.

Some common models include the following:

- NIST CSF
- CIS Top 20
- Microsoft CSAT
- NCSC CAF
- COBIT

Maturity frameworks have ratings often on a 1-5 or 1-4 basis with levels often being similar to as follows:

1. Initial
2. Repeatable
3. Standardized
4. Managed
5. Dynamic



Topics and Areas Covered

This document attempts to cover a wide range of cyber people, process, technology and financial areas. It is broad, but it is not particularly deep. However, I thought it would be good to go through and list some of the topics it covers, these include:

- Business Context
- Strategy
- Governance
- Architecture
- Supply Chain Risk
- Risk Management
- Financial Management
- Secure Design
- Secure Development
- Secure Operations
- Training and Awareness
- Network Security
- Device Security
- Vulnerability Management
- Change and Release Management
- Patch Management
- Data Protection
- Privacy
- Security Monitoring
- Alerting and Reporting
- Incident Response
- Backup and Recovery

Information Security Management Domains

There are more than one standard, framework and guidance documents in the InfoSec and cyber space so if you think there is one ring to rule them go and read the hobbit or lord of the rings (great books but not what we need right now… the eagles will almost certainly not come and save us during a real major cyber incident).

A common industry practise certification broadly aligns to the following domains:

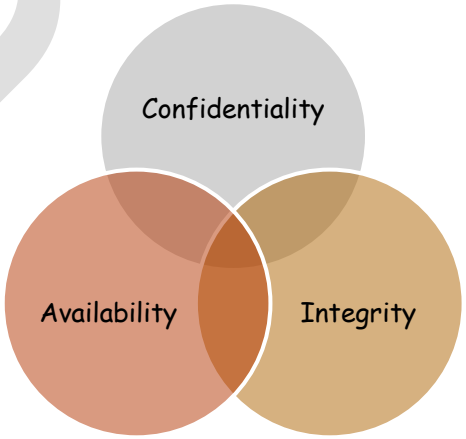
- Security and Risk Management
- Asset Security
- Security Engineering
- Comms/Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

As such you will find these domains represented in this document.

Security spans all areas of the business from governance, legal, finance, marketing, logistics, supply chain through to sales, HR, research and information technology. It is both a broad and deep subject. There is a common misconceptions that security is just a technical arena, and whilst I love technology it's simply not true that is the be all and end all. Technology are the tools which enable us they are not normally the reason for being!

We have to remember that security is concerned with:

- Confidentiality
- Integrity
- Availability



The ACID Test

If you don't have time to go through hundreds of questions and a few pages of my ramblings here's a quick litmus test to run through:

1. Do you have a CISO or SIRO formally defined either as a single role or as part of a role?
2. Do they report to the board?
3. Is there a documented security policy that spans the breadth of the security domains?
4. Do you have process documents that span the security domains?
5. Do you manage change within your business and consider security as part of this change management process?
6. Do you have regular communication between the CISO/SIRO and business process owners?
7. Do you have core evidence that can provided for assurance activities such as?
    a. A risk appetite statement
    b. Asset Registers
    c. Risk Registers
    d. Risk Treatment Plan
    e. Roles and Responsibilities
    f. Vulnerability Reports
    g. Penetration Testing Reports
    h. Incident Logs
    i. Incident Response Plans
    j. Backup and Recovery Plans
    k. Disaster Recovery Plans
    l. Business Continuity Plans
8. Have you conducted a vulnerability assessment in the last quarter?
9. Have you conducted a pentation test within the last year?
10. Does your organisation hold basic security certifications e.g. Cyber Essentials?
11. Does your organisation hold industry standard certifications e.g. ISO27001:2013?
12. Do you have insurance policies which cover cyber risks?

If you answered no to one or more of these I strongly urge you to keep going with this document. The devil is in the detail when it comes to security and risk management, and this document might just be the starting spark on your journey to having a more secure business.

Business/Organisation Context

Provide contextual details as these are important to frame the scenario/context of the organisation and its broad security requirements. Most organisation I've worked with weak security postures and low maturity say statements like "We aren't a bank" and "surely we can't need that". I've worked with banks and it's the same story except regulated industries literally HAVE to have this stuff.

Business Name	
Annual Revenue	
IT Spend as a $ of Revenue	
Industry (Primary Vertical Market)	
Age	
Business Model (e.g. Franchise, Private Org, PLC)	
Number of Employees	
Number of Staff (including contracted staff/temp staff etc)	
Do you provide services to government/military organisations?	
Do you provide services to organisations deemed as 'Critical National Infrastructure'?	
Do you provide services to healthcare providers?	
PCI Requirement (provide level if known)	
List any relevant organisation certifications e.g. ISO27001:2013/Cyber Essentials etc.	
Do you develop software for any of your customers?	
Do you provide any managed services for your customers?	
Do you provide any hosted services for your customers?	
Please list any additional information that is helpful to frame the security context	
Approximately many EU data subject records do you keep within your technology platforms?	

Honesty Box

Time to be brutally honest (or not it's up to you). Do you think your organisation has reasonable and adequate security management focus and controls to protect both your business and customers data/business and people's privacy rights? (tick the appropriate one) at the start, then come back at the end and see if your view still matches (hopefully it does… but don't be surprised if it doesn't)

Date	Phase	Yes	No
	Before Completing Questionnaire		
	After Completing the Questionnaire		

Security Posture

The security posture of an organisation is a description of the level of strength an organisation has to: Identify, Protect, Detect, Respond and Recover from cyber events. I tend to categorise these as follows:

- Strong
- Moderate
- Weak

A security posture much like maturity level is dynamic, it can improve as well as regress.

Leadership, Governance, Strategy and Architecture

1) Do you have board representative responsible for cyber security?
   a) Yes
   b) No
2) Is this formally documented in a job description?
   a) Yes
   b) No
3) Do you have a documented organisational risk register that is reviewed on a regular basis at a board level?
   a) Yes
   b) No
4) Does this include specific cyber risk areas?
   a) Yes
   b) No
5) Do you have reasonable funds, resources and organisational capability focused on cyber security?
   a) Yes
   b) No
6) Do you have a cyber security budget (or can the IT budget be viewed in a way that covers this)?
   a) Yes
   b) No
7) Do you have a documented cyber security strategy and roadmap?
   a) Yes
   b) No
8) Do you have reasonable business, data, and technical documentation to enable cyber security governance and management?
   a) Yes
   b) No
9) Do you have good integration between business operations and security management capabilities?
   a) Yes
   b) No
10) Do you have a baseline set of cyber policies and processes?
   a) Yes
   b) No

Have you written a risk appetite statement to help guide risk management within your organisation?

c) Yes
d) No

11) Do you conduct formal supplier/supply chain risk management and assurance activities?
    a) Yes
    b) No
12) Does your organisation have a cyber insurance policy?
    a) Yes
    b) No
13) Is a data and privacy protection officer formally defined?
    a) Yes
    b) No

Cyber Security Management

Manage

14) Do you have clearly defined cyber roles and responsibilities for the management of areas which includes (but is not limited to) the following:
Risk Management;
Secure Design;
Access Control and Management;
Security Engineering;
Vulnerability Management;
Patch Management;
Penetration Testing;
Threat Intelligence;
Incident Response;
Backup, & Recovery;
Training and Awareness.
    a) Yes
    b) No
15) Do you have a documented company security policy and are staff required to read and comply with this as part of their employment?
    a) Yes
    b) No
16) Is this reviewed, updated and communicated on regular basis?
    a) Yes
    b) No
17) Do you have a baseline set of operational documentation (processes and procedures) for the above areas?
    a) Yes
    b) No
18) Do you have trained staff in these disciplines or a documented mapping of these to outsourced services?
    a) Yes
    b) No
19) Is access to confidential systems and services restricted to authorised personnel only?
    a) Yes
    b) No
20) Do you have a change and authorisation process for authorising administrator access to systems?
    a) Yes

b) No

21) Are staff required to sign confidentiality agreements upon employment?
   a) Yes
   b) No
22) Are checks conducted during the recruitment process (e.g. Reference Checks, CBSS etc.)?
   a) Yes
   b) No
23) Are security and risk management requirements included in employment contracts?
   a) Yes
   b) No
24) Are subcontractors required to sign NDA/Confidentiality agreements?
   a) Yes
   b) No
25) Are suppliers required to sign NDA/Confidentiality agreements?
   a) Yes
   b) No
26) Do you manage, track, log and audit security related operational activity across the business?
   a) Yes
   b) No
27) Do you conduct third party information management system (ISMS) audits?
   a) Yes
   b) No
28) Are supplier contracts reviewed from a security and risk perspective?
   a) Yes
   b) No

Identify

General Purpose Organisation Questions

29) Do you have a documented asset register which records hardware and software assets?
   a) Yes
   b) No
30) A register of third-party systems, services and suppliers is maintained?
   a) Yes
   b) No
31) Has a crown jewel analysis been conducted (have you identified and documented sensitive and critical data locations etc.)
   a) Yes
   b) No
32) Do you have an inventory tool to support asset management?
   a) Yes
   b) No
33) Do you have a documented risk register?
   a) Yes
   b) No
34) Do you have regular risk review meetings?
   a) Yes
   b) No
35) Do you conduct regular vulnerability scanning/assessments?
   a) Yes
   b) No
36) Are critical security updates deployed in a timely manner?
   a) Yes
   b) No
37) Do you conduct and document regular high privilege access reviews and audits?
   a) Yes
   b) No
38) Do you audit systems on a regular basis and ensure obsolete or no longer required user access is disabled?
   a) Yes
   b) No
39) Do you review all non-pre-approved system changes for security implications and impact?
   a) Yes
   b) No

40) Do you conduct regular penetration tests of your internet facing systems?
   a) Yes
   b) No
41) Do you have threat models documented for your environment?
   a) Yes
   b) No
42) Do you have data flow diagrams documented for the environment?
   a) Yes
   b) No
43) Are document handling and information classification policies, processes and procedures documented, communicated and in effect?
   a) Yes
   b) No
44) Do you conduct regular password audits?
   a) Yes
   b) No

45) Do you conduct regular penetration tests of your internal systems?
   a) Yes
   b) No
46) Are all systems and software versions in your environment covered by vendor support? (e.g. OEM, ISV)
47) Are all systems and software appropriately licensed?
   a) Yes
   b) No
48) Are configurations documented and securely stored?
   a) Yes
   b) No
49) Are baselines created and leveraged to conduct system or data integrity checking?
   a) Yes
   b) No
50) Do you have a formal vulnerability disclosure policy and process?
   a) Yes
   b) No
51) Has security.txt been deployed to public facing web services?
   a) Yes
   b) No

Software Development

52)Do you have sufficient architecture and configuration documentation for a security review to be conducted of your software and/or platform?
   a) Yes
   b) No
53)Do you have a secure service/software development lifecycle (SDLC)?
   a) Yes
   b) No
54)Do you conduct code security reviews?
   a) Yes
   b) No
55)Do you conduct security testing conducted as part of your release process?
   a) Yes
   b) No
56)Do you segment developers from being able to make changes to the production system?
   a) Yes
   b) No
57)Do you operate a from a least privilege design?
   a) Yes
   b) No
58)Are good practises around secure software development leveraged? E.g. OWASP
   a) Yes
   b) No
59)Are bugs and defects (including security related ones) tracked in a centralised tracking solution?
   a) Yes
   b) No

Protect

60)Physical controls are in place to protect personnel and assets?
   a) Yes
   b) No
61) Are CCTV systems in place?
   a) Yes
   b) No
62)Are alarm systems in place?
   a) Yes
   b) No
63)Are door access control systems in place?
   a) Yes
   b) No
64)Are computers in public areas protected by physical controls (e.g. Kensington locks)
   a) Yes
   b) No
65)Do you implement a strong authentication policy for computer systems?
   a) Yes
   b) No
66)Are account lockout mechanisms in place to prevent brute force attacks?
   a) Yes
   b) No
67)Where possible do you implement multi-factor authentication?
   a) Yes
   b) No
68)Are default passwords for systems changed?
   a) Yes
   b) No
69)Do your systems leverage role-based access?
   a) Yes
   b) No
70)Do you harden network devise, servers, PCs and mobile devices to a known good standard (e.g. vendor guidance, or CIS controls etc.)?
   a) Yes
   b) No
71) Where appropriate do you leverage redundancy equipment or services (e.g. RAID, Load Balancing, Clustering etc.)
   a) Yes
   b) No

72) Are host-based firewalls enabled where present?
   a) Yes
   b) No
73) Do you deploy antimalware/antivirus services to all servers, PCs and applicable devices (where the technology allows)?
   a) Yes
   b) No
74) Have you enabled application allow listing?
   a) Yes
   b) No
75) Have you restricted users (that includes all staff roles) from having administrator rights on endpoints for regular day to day use?
   a) Yes
   b) No
76) Do you disable Office macros for users who do not require them for their job?
   a) Yes
   b) No
77) Do you encrypt devices physical storage?
   a) Yes
   b) No
78) Do you disable removable device access where it isn't required?
   a) Yes
   b) No
79) Do you restrict access to system administration interfaces (e.g. firewalls, servers etc.)?
   a) Yes
   b) No
80) Do you block risky egress (outbound network traffic e.g. TCP 445 (SMB) from corporate networks and devices?
   a) Yes
   b) No
81) Is protective DNS in place?
   a) Yes
   b) No
82) Is web content filtering/proxying in place?
   a) Yes
   b) No

Are screens configured to lock automatically when unattended?

c) Yes
d) No

83) Are critical business systems and data protected by a backup and recovery solution?

a) Yes
b) No

84) Are backups encrypted?

a) Yes
b) No

85) Are backup copies also held offsite?

a) Yes
b) No

86) Are backups servers hardened against attack and configured off the domain?

a) Yes
b) No

88) Are perimeter firewalls in place?
   a) Yes
   b) No
89) Are secure and hardened remote access services in place?
   a) Yes
   b) No
90) Do you have a perimeter firewall that supports IPS features and are they enabled?
   a) Yes
   b) No
91) Do you segment your network devices and restrict traffic flows to what is required?
   a) Yes
   b) No
92) Do you use strong wireless authentication protocols and keys?
   a) Yes
   b) No
93) Do you ensure guest Wi-Fi is isolated from the corporate network?
   a) Yes
   b) No
94) Do your systems get administered with privileged access workstations (dedicated and hardened administration devices)?
   a) Yes
   b) No
95) Is remote access to systems configured to use a VPN or similar service?
   a) Yes
   b) No
96) Are remote access services protected via multi-factor authentication?
   a) Yes
   b) No
97) Is confidential/sensitive data protected in transit (e.g. using TLS/IPSEC)
   a) Yes
   b) No
98) Is confidential/sensitive data protected at rest (e.g. disk or file encryption)
   a) Yes
   b) No
99) Do you leverage Information Rights Management or Data Loss Prevention services?
   a) Yes
   b) No

Do you leverage e-discovery services?

c) Yes
d) No

100) Are secure data wipes conducted on service retirement?
a) Yes
b) No

101) Are physical assets disposed of in a secure manner?
a) Yes
b) No

102) Are assets disposed of safely with regard to environmental safety and standards? E.g. WEE
a) Yes
b) No

103) Do you manage Mobile device's via MDM services?
a) Yes
b) No

104) DO you prevent mobile devices from being rooted or are rooted devise prohibited from accessing systems?
a) Yes
b) No

105) Are Servers and PCs are managed via a remote management solution?
a) Yes
b) No

106) Are Patch management systems in place to centrally manage operating system patched?
a) Yes
b) No

107) Patch management systems are in place to centrally manage third party software components.
a) Yes
b) No

Detect

108) Do you monitor services for availability?
   a) Yes
   b) No
109) Do you monitor service components for availability?
   a) Yes
   b) No
110) Do you centrally collect, analyse and alert on security events (e.g. do you use a SIEM or other audit log analysis service)?
   a) Yes
   b) No
111) Do you monitor process activation, file level changes, group membership changes on server and PC devices (e.g. use SYSMON or similar)?
   a) Yes
   b) No
112) Do you monitor your attack surface for vulnerabilities and exposed risky services?
   a) Yes
   b) No
113) Do you monitor systems for anomalous events (e.g. unrealistic geo travel, nonstandard logon patterns etc.)?
   a) Yes
   b) No
114) Do you monitor your domains for known breaches (e.g. using "Have I been pwned?" or similar?)
   a) Yes
   b) No
115) Do you monitor vendor feeds for known vulnerabilities?
   a) Yes
   b) No
116) Do changes to high privileges access group memberships create alerts?
   a) Yes
   b) No
117) Do you keep log files in a separate system and retain logs for reasonable period for later review?
   a) Yes
   b) No

118) Have you deployed decoys or honeypots?
   a) Yes
   b) No
119) Have you deployed canaries?
   a) Yes
   b) No
120) Do you conduct RED/PURPLE team simulations to improve detection and response capabilities?
   a) Yes
   b) No

Respond

121) Do you have a documented incident response process?
   a) Yes
   b) No
122) Does your incident response process include interfaces to other areas such as legal, marketing, communications, exec boards etc?
   a) Yes
   b) No
123) Do you practise incident response drills?
   a) Yes
   b) No
124) Do you have mechanisms for collecting evidence for analysis during an incident?
   a) Yes
   b) No
125) Do you conduct a lesson learnt review after an incident and use the learnings to improve the security posture of the service and response efforts?
   a) Yes
   b) No
126) Do you change passwords when breaches are suspected or identified?
   a) Yes
   b) No
127) Does your response team have a warm standby response kit?
   a) Yes
   b) No
128) Have secure out of band channels of communication been agreed?
   a) Yes
   b) No

Recover

129) Do you have a documented recovery plan for normal incidents (e.g. loss of a single server at a site)?
   a) Yes
   b) No

130) Do you have a documented recovery plan for major loss of services at a single site?
   a) Yes
   b) No

131) Do you have a documented recovery plan for major loss of technology services across the enterprise?
   a) Yes
   b) No

132) Do you conduct drills against your recovery plans on a regular basis? (in line with incident category e.g. minor, routine, major)
   a) Yes
   b) No

133) Can you recover your business assets if all your online services are breached?
   a) Yes
   b) No

134) Do you keep vital business information in escrow or similar (if required subject to the nature of the business and the services it provides)?
   a) Yes
   b) No

135) Do you report your findings from incidents to the board?
   a) Yes
   b) No

136) Where applicable to you report data breaches to the regulatory body? (e.g. ICO)
   a) Yes
   b) No

137) Where required by law are relevant law enforcement agencies engaged (e.g. the NCA)?
   a) Yes
   b) No

138) When and if appropriate, are country cyber response services contacted (e.g. Country CIRT/CERT teams)?
   a) Yes
   b) No

139) Where appropriate data subjects are informed about a breach, the impact and any recommended actions they should take, alongside actions the organisation is taking?
   a) Yes
   b) No

140) Data from incidents is shared with the security community (threat intelligence) to improve the industry etc.
   a) Yes
   b) No

Upon Completion

Great you have now conducted a very brief and high-level review of your security posture. Now you probably expect there to be a magic list of things to do, a product to buy or some Blinky box that will solve your gaps. It's likely in the majority of cases that won't be the case.

Cyber security and its management within a business requires resources, leadership, effort and normally a fair level of change. It's a journey not a quick fix. There are of course a range of things that can be done tactically and then there are more strategic long-term activities. These do vary depending upon your organisation's goals, objectives and context of the scenario.

Let's not just take my word for it

Who am I to say what good is or is not? Some might say I'm experienced and knowledgeable, but you know that's just an opinion. So, let's compare this small work to an industry standard. Since this is aimed at a 101 style let's go with Cyber Essentials:

Cyber Essentials Reference	Covered	Section/s
A4.1	Yes	Protect
A4.2	Yes	Protect
A4.3	Yes	Protect
A4.4	Yes	Detect, Respond
A4.5	Yes	Protect
A4.6	Yes	Detect
A4.8	Yes	Protect
A4.9	Yes	Protect
A4.11	Yes	Protect
A5.1	Yes	Protect
A5.2	Yes	Protect
A5.3	Yes	Protect
A5.4	Yes	Protect
A5.6	Yes	Protect
A5.7	Yes	Detect, Respond
A5.8, A5.9	Yes	Protect
A5.10	Yes	Protect
A6.1	Yes	Identify
A6.2	Yes	Identify
A6.3	Yes	Identify
A6.4	Yes	Manage, Identify, Protect
A6.5	Yes	Manage, Identify, Protect
A6.6	Yes	Identify
A7.1	Yes	Management
A7.2	Yes	Protect
A7.3	Yes	Identify
A7.4	Yes	Identify
A7.5	Yes	Manage
A7.6	Yes	Protect
A7.7	Yes	Protect
A7.8	Yes	Manage, Identify, Protect, Detect

A7.9	Yes	Manage, Identify, Protect, Detect
A7.10 & A7.11	Yes	Protect
A8.1, A8.2, A8.3, A8.4	Yes	Protect
A8.5	Yes	Manage, Protect
A8.6	Yes	Manage, Protect

It must be noted that the wording in this document and cyber essentials is not a one to one mapping some areas are implied. E.g. hardened configurations in protection would cover areas in cyber essentials.

To compare breadth and depth cyber essentials has <50 control and process questions. This document has > 80. That's not a slant on cyber essentials, far from it. It's a great foundational certification and I strongly recommend organisations achieve it. It does not however cover all the areas required to protect your organisations systems and data.

NIST CSF Analysis

This NIST CSF has 109 sections in its core framework workbook at the time of writing. This document now has 140 questions and whilst it doesn't perfectly align with the CSF (the CSF is more detail orientated) it does very much so in the spirit of its nature. THE NIST CSF references a range of standards and is in practise far more detailed (I'm not trying to replace any of that great stuff in any other framework etc.).

ISO27001:2013

Lastly because the point is demonstrated already we will ensure that this document is in alignment with ISO27001:2013. ISO27001 contains 11 Control Groups and in these 161 Control Objectives. ISO has far more detail around physical controls, human resources etc. than this questionnaire but again the general spirit is in alignment.

SOC2 Principals

SOC2 has 302 points of focus which are summarised into 17 principles.

COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

We haven't conducted a deep analysis comparison, but the general spirit of this document would be in alignment with SOC2 (in my opinion)

Going Further

As I've gone on this journey to make a light touch view I'm realising that to the un-initiated this in itself might seem like a lot, but hopefully once you have gone through the process you will realise that actually we just scratched the surface of information/cyber security (let alone privacy). Taking this further would normally look like this:

Expanding the details, normally by leveraging additional frameworks (not just InfoSec ones) such as:

- ITIL
- COBIT
- TOGAF/SABSA/ZACHMAN (Architecture frameworks)

Go deeper into each area. I'll give you an example of this. CREST have an incident response maturity assessment which is over 100 questions long. Now this looks into linkages between incident response and other areas (not surprisingly all these things are connected (or at least they should be!).

A second view on this as well is that simply say yes doesn't really provide an evidence-based approach (it's just an opinion) so to expand this think about evidence collection.

If you want to see a formal framework for different styles of assessment it's worth taking a read of SCAMPI from CMMI (it's not a quick read, to be honest most frameworks aren't fast to read or understand).

You are the new CISO now what?

Why have I put in a reference to a new CISO in this document? Good question. Well I think that's it's entirely appropriate not only for CEO's, COO's to understand what they are asking someone to for but also for new CISO's/Security Leaders/Managers to get a view on why this questions are and other assessments are useful tools to support new appointments into a CISO or other related role.

Welcome to the jungle

Now every organisation is different, so this isn't a one size fits all (most things in life 'depend' up on a great many things) but this is going to talk through some common things that people will likely want to consider doing when they get into a new environment. Your actual activity will be different depending upon the size, scale, complexity, maturity and culture of the organisation you are in.

The First 100 Days

For starters let's see what 100 days is, well in business terms that's about 3 months (shockingly this is usually an organisation minimum probationary period). Why 3 months? Well I can only speak for myself, but it takes about that long to start to get a grip on things (and if this isn't true why do you have probationary periods that long?). This isn't an in depth 100-day plan in this document but it's a snippet to get you thinking!

High Level Timeline

1-10	10-20	20-30	30-40	50-60	70-80	80-90	100
Plan	Discover	Assess	Change	Change	Monitor	Monitor	Grow

Activities

- Plan to Plan
    - Running in without a plan isn't a great idea, the first plan should be to plan your entry and activities.
- Understand the current state
    - Conduct recon against the organisation
    - Know your stakeholders
    - Understand your high-level objectives
    - Discover the business
    - Review what is and what was before
    - Baseline the current state
        - Use questionnaires;
        - Audits;
        - maturity Assessments;
        - Health checks;
        - Vulnerability scans;
        - Network discovers;
        - Penetration tests etc.
- Create a tactical and strategic plan (strategy/roadmap etc.)
    - Develop a roadmap
    - Look at quick tactical wins
    - Look at longer term strategic objectives
    - Put key events into your plan (there might be mandatory audits etc.)
    - Ensure the plan links to business objectives and activity
- Conduct tactical activities
    - Go after low hanging fruit
    - Formulate teams/working groups etc.
- Communicate
    - Ensure you communicate with key stakeholders
    - Ensure you communicate with your manager
    - Work with the team
- Monitor and Assess change
    - Organisational change requires a steady hand you can't do too much at once and you need to monitor changes, this is true as well for systems-based changes.

Conclusion

It feels like every day/week/month these days that we hear about a significant cyber event. I've been planning designing, building, operating and advising in the technology world for over 20 years and one thing is fairly obvious to me, building and deploying technology is not easy let alone securing it. We have as a human race deployed technology and made it ubiquitous in our lives, but we have done that in a way and at a pace that has left people and organisations at risk.,

This tool is just that, a simple tool to help you understand a little about your security posture. I wrote this in a day, but it's got a fair bit of experience put into it. Whilst when you read this it will have been reviewed, cross referenced against frameworks and good practises etc. I wrote this part before all that had occurred. Let's hope the QA team don't rip it to shreds but also jokes aside I want people to know these weren't plucked from thin air, this comes from experience (and it's been checked for sanity against industry standard frameworks such as cyber essentials and NIST CSF).

You are probably wondering why I haven't written a 3-step plan or some other exec style roadmap at the end. It's because each organising is at its own position and if you think a 3-step single page is going to get you there you're probably missing the point. Hard work, attention to detail, enabling teams and implementing good practises takes time and is usually not a 3-step process.

I hope people find at least some of this useful. I have used the approach and style that I've had success with over the years, and it's an intro into the wider world or far more in-depth analysis.

May the force be with you!

- mRr3b00t

N.B., I wrote this in comic sans because it's funny! If you live life without a smile are you really living at all?

[Page Intentionally Blank]

Appendices

Appendix A – References

Supply Chain Assurance Questions from NCSC

https://www.ncsc.gov.uk/guidance/supplier-assurance-questions

ICO Adequacy Guidance

https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/what-does-adequacy-mean/

NCSC CAF Assessment Framework

https://www.ncsc.gov.uk/collection/caf

ISO 27001:2013

https://www.iso.org/standard/54534.html

CISSP

https://www.isc2.org/Certifications/CISSP

ITIL

https://www.axelos.com/best-practice-solutions/itil

NCSC Cloud Security Principles

https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

NIST CSF

https://www.nist.gov/cyberframework

NIST SP 800 Series

https://csrc.nist.gov/publications/sp800