3. CYBERSECURITY AUDIT CHECKLIST

1	**ID. ASSESS HOW WELL CONTEXT IS UNDERSTOOD**	DO	DN	NA	
2	**ID.AM Assess how well relevant assets are understood.**	DO	DN	NA	
3	ID.AM-1 Assess how well physical devices and systems are understood.	DO	DN	NA	
4	ID.AM-2 Assess how well software platforms and apps are understood.	DO	DN	NA	
5	ID.AM-3 Assess how well communication and data flows are understood.	DO	DN	NA	
6	ID.AM-4 Assess how well external information systems are understood.	DO	DN	NA	
7	ID.AM-5 Assess how well security priorities and resources are understood.	DO	DN	NA	
8	ID.AM-6 Assess how well security roles and responsibilities are understood.	DO	DN	NA	
9	**ID.BE Assess how well business environment is understood.**	DO	DN	NA	
10	ID.BE-1 Assess how well suppliers and supply chains are understood.	DO	DN	NA	
11	ID.BE-2 Assess how well your infrastructure environment is understood.	DO	DN	NA	
12	ID.BE-3 Assess how well cybersecurity issues and priorities are understood.	DO	DN	NA	
13	ID.BE-4 Assess how well functions and dependencies are understood.	DO	DN	NA	
14	ID.BE-5 Assess how well resilience requirements are understood.	DO	DN	NA	
15	**ID.GV Assess how well governance issues are understood.**	DO	DN	NA	
16	ID.GV-1 Assess how well your cybersecurity policy is understood.	DO	DN	NA	
17	ID.GV-2 Assess how well cybersecurity responsibilities are understood.	DO	DN	NA	
18	ID.GV-3 Assess how well legal and regulatory requirements are understood.	DO	DN	NA	
19	ID.GV-4 Assess how well your risk management processes are understood.	DO	DN	NA	
20	**ID.RA Assess how well threats and risks are understood.**	DO	DN	NA	
21	ID.RA-1 Assess how well vulnerabilities are understood.	DO	DN	NA	
22	ID.RA-2 Assess how well threat intelligence is understood.	DO	DN	NA	

23	ID.RA-3 Assess how well cybersecurity threats are understood.	DO	DN	NA	
24	ID.RA-4 Assess how well impacts and likelihoods are understood.	DO	DN	NA	
25	ID.RA-5 Assess how well security risks are defined and understood.	DO	DN	NA	
26	ID.RA-6 Assess how well treatments and responses are understood.	DO	DN	NA	
27	**ID.RM Assess how well risk management is understood.**	DO	DN	NA	
28	ID.RM-1 Assess how well risk processes are understood.	DO	DN	NA	
29	ID.RM-2 Assess how well risk tolerances are understood.	DO	DN	NA	
30	ID.RM-3 Assess how well risk environment is understood.	DO	DN	NA	
31	**ID.SC Assess how well supply chains are understood.**	DO	DN	NA	
32	ID.SC-1 Assess how well supply chain risk processes are understood.	DO	DN	NA	
33	ID.SC-2 Assess how well supply chain risk assessments are understood.	DO	DN	NA	
34	ID.SC-3 Assess how well supply chain security contracts are understood.	DO	DN	NA	
35	ID.SC-4 Assess how well supplier and partner performance is understood.	DO	DN	NA	
36	ID.SC-5 Assess how well supply chain response and recovery is understood.	DO	DN	NA	
37	**PR. ASSESS HOW WELL ASSETS ARE PROTECTED**	DO	DN	NA	
38	**PR.AC Assess how well access is being managed.**	DO	DN	NA	
39	PR.AC-1 Assess how well identities are being controlled.	DO	DN	NA	
40	PR.AC-2 Assess how well physical access is being controlled.	DO	DN	NA	
41	PR.AC-3 Assess how well remote access is being controlled.	DO	DN	NA	
42	PR.AC-4 Assess how well authorizations are being controlled.	DO	DN	NA	
43	PR.AC-5 Assess how well network access is being controlled.	DO	DN	NA	
44	PR.AC-6 Assess how well identity proof is being controlled.	DO	DN	NA	
45	PR.AC-7 Assess how well access risk is being controlled.	DO	DN	NA	

46	**PR.AT Assess how well awareness is being managed.**	DO	DN	NA	
47	PR.AT-1 Assess how well users are made aware of their security duties.	DO	DN	NA	
48	PR.AT-2 Assess how well privileged users are made aware of their duties.	DO	DN	NA	
49	PR.AT-3 Assess how well stakeholders are made aware of security duties.	DO	DN	NA	
50	PR.AT-4 Assess how well executives are made aware of security duties.	DO	DN	NA	
51	PR.AT-5 Assess how well security personnel are made aware of duties.	DO	DN	NA	
52	**PR.DS Assess how well data security is being managed.**	DO	DN	NA	
53	PR.DS-1 Assess how well data-at-rest is being managed.	DO	DN	NA	
54	PR.DS-2 Assess how well data-in-transit is being managed.	DO	DN	NA	
55	PR.DS-3 Assess how well asset transfers are being managed.	DO	DN	NA	
56	PR.DS-4 Assess how well data availability is being managed.	DO	DN	NA	
57	PR.DS-5 Assess how well data breaches are being managed.	DO	DN	NA	
58	PR.DS-6 Assess how well data integrity is being managed.	DO	DN	NA	
59	PR.DS-7 Assess how well development is being managed.	DO	DN	NA	
60	PR.DS-8 Assess how well hardware is being managed.	DO	DN	NA	
61	**PR.IP Assess how well information is being managed.**	DO	DN	NA	
62	PR.IP-1 Assess how well security principles are being adopted.	DO	DN	NA	
63	PR.IP-2 Assess how well system life cycle models are being used.	DO	DN	NA	
64	PR.IP-3 Assess how well change controls are being implemented.	DO	DN	NA	
65	PR.IP-4 Assess how well information backups are being performed.	DO	DN	NA	
66	PR.IP-5 Assess how well operating environment is being controlled.	DO	DN	NA	
67	PR.IP-6 Assess how well data destruction policies are being followed.	DO	DN	NA	

Now that you've seen a sample of our approach, please consider purchasing our complete product:

***Praxiom's Plain English Cybersecurity Audit Tool (*Title 61).**

Title 61 contains both a general audit checklist (see above) and a detailed set of cybersecurity audit questions (see pdf).

If you purchase our Plain English Audit Tool, you'll find that it's detailed, exhaustive, and easy to understand. We guarantee it. Title 61 comes in both MS Word and pdf file formats and is 94 pages long.

How to Place an Order: https://www.praxiom.com/orders.htm