PRAXIOM'S PLAIN ENGLISH CYBERSECURITY AUDIT TOOL

PR. ASSESS HOW WELL ASSETS ARE PROTECTED

PR.AC ASSESS HOW WELL ACCESS IS BEING MANAGED

1	Do you limit access to your organization's assets and facilities?	Y	N	X	
2	Do you limit access to your organization's physical assets and facilities?	Y	N	X	
3	Do you allow only authorized users to have access to physical assets and facilities?	Y	N	X	
4	Do you allow only authorized devices to have access to physical assets and facilities?	Y	N	X	
5	Do you allow only authorized processes to have access to physical assets and facilities?	Y	N	X	
6	Do you limit access to your organization's logical assets and facilities?	Y	N	X	
7	Do you allow only authorized users to have access to logical assets and facilities?	Y	N	X	
8	Do you allow only authorized devices to have access to logical assets and facilities?	Y	N	X	
9	Do you allow only authorized processes to have access to logical assets and facilities?	Y	N	X	
10	Do you manage access to your organization's assets and facilities?	Y	N	X	
11	Do you manage access commensurate with the risk being taken?	Y	N	X	
12	Do you manage access to your organization's physical assets and facilities?	Y	N	X	
13	Do you consider the risk being taken when physical access is granted to users?	Y	N	X	
14	Do you consider the risk being taken when physical access is granted to devices?	Y	N	X	
15	Do you consider the risk being taken when physical access is granted to processes?	Y	N	X	
16	Do you manage access to your organization's logical assets and facilities?	Y	N	X	
17	Do you consider the risk being taken when logical access is granted to users?	Y	N	X	
18	Do you consider the risk being taken when logical access is granted to devices?	Y	N	X	
19	Do you consider the risk being taken when logical access is granted to processes?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

PR. ASSESS HOW WELL ASSETS ARE PROTECTED

PR.AC-1 ASSESS HOW WELL IDENTITIES ARE BEING CONTROLLED					
20	Do you control identities and credentials for authorized users?	Y	N	X	
21	Do you control the verification of user identities and credentials?	Y	N	X	
22	Do you control the issuance of user identities and credentials?	Y	N	X	
23	Do you control the revocation of user identities and credentials?	Y	N	X	
24	Do you control the auditing of user identities and credentials?	Y	N	X	
25	Do you control identities and credentials for authorized devices?	Y	N	X	
26	Do you control the verification of device identities and credentials?	Y	N	X	
27	Do you control the issuance of device identities and credentials?	Y	N	X	
28	Do you control the revocation of device identities and credentials?	Y	N	X	
29	Do you control the auditing of device identities and credentials?	Y	N	X	
30	Do you control identities and credentials for authorized processes?	Y	N	X	
31	Do you control the verification of process identities and credentials?	Y	N	X	
32	Do you control the issuance of process identities and credentials?	Y	N	X	
33	Do you control the revocation of process identities and credentials?	Y	N	X	
34	Do you control the auditing of process identities and credentials?	Y	N	X	
PR.AC-2 ASSESS HOW WELL PHYSICAL ACCESS IS BEING CONTROLLED					
35	Do you control physical access to your organization's assets and associated facilities?	Y	N	X	
36	Do you manage physical access to your organization's assets and associated facilities?	Y	N	X	
37	Do you protect physical access to your organization's assets and associated facilities?	Y	N	X	
38	Do you protect physical assets that contain either sensitive or critical information?	Y	N	X	
39	Do you allow only authorized users to access these physical assets and facilities?	Y	N	X	
40	Do you use entry controls to allow only authorized people to have access?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

PR. ASSESS HOW WELL ASSETS ARE PROTECTED

PR.AC-3 ASSESS HOW WELL REMOTE ACCESS IS BEING CONTROLLED					
41	Do you control remote access to your organization's assets and associated facilities?	Y	N	X	
42	Do you manage remote access to your organization's assets and associated facilities?	Y	N	X	
43	Do you establish remote access control policies and procedures for your organization?	Y	N	X	
44	Do you establish remote access restriction, connection, and configuration requirements?	Y	N	X	
45	Do you establish appropriate usage restrictions and requirements for mobile devices?	Y	N	X	
PR.AC-4 ASSESS HOW WELL AUTHORIZATIONS ARE BEING CONTROLLED					
46	Do you control how access permissions and authorizations are managed?	Y	N	X	
47	Do you incorporate "separation of duties" and "least privilege" principles?	Y	N	X	
48	Do you protect assets by segregating conflicting duties and responsibilities?	Y	N	X	
49	Do you protect assets by granting access privileges no higher than necessary?	Y	N	X	
50	Do you grant access privileges no higher than what is needed to do assigned tasks?	Y	N	X	
PR.AC-5 ASSESS HOW WELL NETWORK ACCESS IS BEING CONTROLLED					
51	Do you protect and control the integrity of your organization's networks?	Y	N	X	
52	Do you consider using network segregation to control network access and integrity?	Y	N	X	
53	Do you consider using network segmentation to control network access and integrity?	Y	N	X	
PR.AC-6 ASSESS HOW WELL IDENTITY PROOF IS BEING CONTROLLED					
54	Do you control the unique identities of your users, devices, and processes?	Y	N	X	
55	Do you control how identities of users, devices, and processes are proofed?	Y	N	X	
56	Do you control how identities of users, devices, and processes are bound?	Y	N	X	
57	Do you control how identities of users, devices, and processes are asserted?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

PR.AC-7 ASSESS HOW WELL ACCESS RISK IS BEING CONTROLLED					
58	Do you control the authentication of users who have access to physical and logical assets?	Y	N	X	
59	Do you authenticate these users commensurate with the transaction risk being taken?	Y	N	X	
60	Do you consider the security, privacy, and other risks that individuals are exposed to?	Y	N	X	
61	Do you consider the risk that your organization is taking when users are authenticated?	Y	N	X	
62	Do you control the authentication of devices that have access to physical and logical assets?	Y	N	X	
63	Do you authenticate these devices commensurate with the transaction risk being taken?	Y	N	X	
64	Do you consider the risk that your organization is taking when devices are authenticated?	Y	N	X	
65	Do you control the authentication of processes that have access to physical and logical assets?	Y	N	X	
66	Do you authenticate these processes commensurate with the transaction risk being taken?	Y	N	X	
67	Do you consider the risk that your organization is taking when processes are authenticated?	Y	N	X	
PR.AT ASSESS HOW WELL AWARENESS IS BEING MANAGED					
68	Do you provide cybersecurity awareness services to personnel and partners?	Y	N	X	
69	Do you make your organization's personnel aware of their cybersecurity responsibilities?	Y	N	X	
70	Do you make personnel aware of the cybersecurity policies that they must respect?	Y	N	X	
71	Do you make personnel aware of the cybersecurity procedures that they must follow?	Y	N	X	
72	Do you make personnel aware of the cybersecurity agreements that they must implement?	Y	N	X	
73	Do you make your organization's partners aware of their cybersecurity responsibilities?	Y	N	X	
74	Do you make partners aware of the cybersecurity policies that they must respect?	Y	N	X	
75	Do you make partners aware of the cybersecurity procedures that they must follow?	Y	N	X	
76	Do you make partners aware of the cybersecurity agreements that they must implement?	Y	N	X	
77	Do you provide cybersecurity training services to personnel and partners?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

78	Do you teach personnel how to perform their cybersecurity duties and responsibilities?	Y	N	X	
79	Do you teach personnel how to perform their work in accordance with related policies?	Y	N	X	
80	Do you teach personnel how to perform their work in accordance with related procedures?	Y	N	X	
81	Do you teach personnel how to perform their work in accordance with related agreements?	Y	N	X	
82	Do you teach partners how to perform their cybersecurity duties and responsibilities?	Y	N	X	
83	Do you teach partners how to perform their work in accordance with related policies?	Y	N	X	
84	Do you teach partners how to perform their work in accordance with related procedures?	Y	N	X	
85	Do you teach partners how to perform their work in accordance with related agreements?	Y	N	X	
PR.AT-1 ASSESS HOW WELL USERS ARE MADE AWARE OF THEIR SECURITY DUTIES					
86	Do you provide cybersecurity awareness services to your organization's users?	Y	N	X	
87	Do you make your organization's users aware of their cybersecurity responsibilities?	Y	N	X	
88	Do you make users aware of the cybersecurity policies that they must respect?	Y	N	X	
89	Do you make users aware of the cybersecurity procedures that they must follow?	Y	N	X	
90	Do you make users aware of the cybersecurity agreements that they must implement?	Y	N	X	
91	Do you provide cybersecurity training services to your organization's users?	Y	N	X	
92	Do you teach all users how to perform their cybersecurity duties and responsibilities?	Y	N	X	
93	Do you teach users how to perform their work in accordance with related policies?	Y	N	X	
94	Do you teach users how to perform their work in accordance with related procedures?	Y	N	X	
95	Do you teach users how to perform their work in accordance with related agreements?	Y	N	X	
PR.AT-2 ASSESS HOW WELL PRIVILEGED USERS ARE MADE AWARE OF THEIR DUTIES					
96	Do you provide cybersecurity awareness services to all privileged users?	Y	N	X	
97	Do you make privileged users aware of their cybersecurity responsibilities?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

98	Do you make privileged users aware of the policies that they must respect?	Y	N	X	
99	Do you make privileged users aware of the procedures that they must follow?	Y	N	X	
100	Do you make privileged users aware of the agreements that they must implement?	Y	N	X	
101	Do you provide cybersecurity training services to all privileged users?	Y	N	X	
102	Do you teach privileged users how to perform cybersecurity duties and responsibilities?	Y	N	X	
103	Do you teach privileged users how to perform work in accordance with related policies?	Y	N	X	
104	Do you teach privileged users how to perform work in accordance with related procedures?	Y	N	X	
105	Do you teach privileged users how to perform work in accordance with related agreements?	Y	N	X	
PR.AT-3 ASSESS HOW WELL STAKEHOLDERS ARE MADE AWARE OF SECURITY DUTIES					
106	Do you make sure that third-party stakeholders understand their cybersecurity obligations?	Y	N	X	
107	Do you make sure that partners understand their cybersecurity roles and responsibilities?	Y	N	X	
108	Do you make partners aware of the cybersecurity policies that must be applied?	Y	N	X	
109	Do you make partners aware of the cybersecurity procedures that must be followed?	Y	N	X	
110	Do you make partners aware of the cybersecurity agreements that must be implemented?	Y	N	X	
111	Do you make sure that suppliers understand their cybersecurity roles and responsibilities?	Y	N	X	
112	Do you make suppliers aware of the cybersecurity policies that must be applied?	Y	N	X	
113	Do you make suppliers aware of the cybersecurity procedures that must be followed?	Y	N	X	
114	Do you make suppliers aware of the cybersecurity agreements that must be implemented?	Y	N	X	
115	Do you make sure that customers understand their cybersecurity roles and responsibilities?	Y	N	X	
116	Do you make customers aware of the cybersecurity policies that must be applied?	Y	N	X	
117	Do you make customers aware of the cybersecurity procedures that must be followed?	Y	N	X	
118	Do you make customers aware of the cybersecurity agreements that must be implemented?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

PR.AT-4 ASSESS HOW WELL EXECUTIVES ARE MADE AWARE OF SECURITY DUTIES					
119	Do you make sure that your senior executives understand their cybersecurity functions?	Y	N	X	
120	Do you make sure that executives understand their cybersecurity roles and responsibilities?	Y	N	X	
121	Do you make senior executives aware of the cybersecurity policies that must be applied?	Y	N	X	
122	Do you make senior executives aware of the cybersecurity procedures that must be followed?	Y	N	X	
123	Do you make senior executives aware of the cybersecurity agreements that must be implemented?	Y	N	X	
PR.AT-5 ASSESS HOW WELL SECURITY PERSONNEL ARE MADE AWARE OF DUTIES					
124	Do you make sure that physical security personnel understand their roles and responsibilities?	Y	N	X	
125	Do you make physical security personnel aware of the policies that must be applied?	Y	N	X	
126	Do you make physical security personnel aware of the procedures that must be followed?	Y	N	X	
127	Do you make physical security personnel aware of the agreements that must be implemented?	Y	N	X	
128	Do you make sure that cybersecurity personnel understand their roles and responsibilities?	Y	N	X	
129	Do you make cybersecurity personnel aware of the policies that must be applied?	Y	N	X	
130	Do you make cybersecurity personnel aware of the procedures that must be followed?	Y	N	X	
131	Do you make cybersecurity personnel aware of the agreements that must be implemented?	Y	N	X	
PR.DS ASSESS HOW WELL DATA SECURITY IS BEING MANAGED					
132	Do you protect the confidentiality, integrity, and availability of your organization's data?	Y	N	X	
133	Do you protect the confidentiality, integrity, and availability of your organization's records?	Y	N	X	
134	Do you manage your records using methods that are consistent with your risk strategy?	Y	N	X	
135	Do you protect the confidentiality, integrity, and availability of your organization's information?	Y	N	X	
136	Do you manage your information using methods that are consistent with your risk strategy?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

PR.DS-1 ASSESS HOW WELL DATA-AT-REST IS BEING MANAGED					
137	Do you protect the confidentiality, integrity, and availability of your data-at-rest?	Y	N	X	
138	Do you protect your data-at-rest using methods that are consistent with your risk strategy?	Y	N	X	
139	Do you consider removing your data-at-rest from online storage and putting it off-line?	Y	N	X	
140	Do you consider using cryptographic tools to prevent unauthorized access to data-at-rest?	Y	N	X	
PR.DS-2 ASSESS HOW WELL DATA-IN-TRANSIT IS BEING MANAGED					
141	Do you protect the confidentiality, integrity, and availability of your data-in-transit?	Y	N	X	
142	Do you protect your data-in-transit using methods that are consistent with your risk strategy?	Y	N	X	
143	Do you consider using transfer policies and procedures to protect and preserve data-in-transit?	Y	N	X	
144	Do you consider using trusted communication paths to protect and preserve data-in-transit?	Y	N	X	
145	Do you consider using cryptographic technologies to protect and preserve data-in-transit?	Y	N	X	
146	Do you consider using cryptographic tools to prevent unauthorized access to data-in-transit?	Y	N	X	
147	Do you consider using cryptographic tools to detect unauthorized modification of data-in-transit?	Y	N	X	
148	Do you consider using cryptographic tools to prevent unauthorized disclosure of data-in-transit?	Y	N	X	
149	Do you consider using cryptographic mechanisms to conceal or randomize communications?	Y	N	X	
150	Do you consider using cryptographic mechanisms to protect message externals (e.g., headers)?	Y	N	X	
PR.DS-3 ASSESS HOW WELL ASSET TRANSFERS ARE BEING MANAGED					
151	Do you manage assets throughout transfer, removal, and disposition?	Y	N	X	
152	Do you use asset management methods consistent with your risk?	Y	N	X	
153	Do you consider formally managing the transfer of your assets?	Y	N	X	
154	Do you consider controlling how asset transfers are authorized?	Y	N	X	
155	Do you consider controlling how asset transfers are monitored?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

156	Do you consider controlling how asset transfers are recorded?	Y	N	X	
157	Do you consider formally managing the movement of assets?	Y	N	X	
158	Do you consider controlling how assets enter your facilities?	Y	N	X	
159	Do you consider controlling how asset entry is authorized?	Y	N	X	
160	Do you consider controlling how asset entry is monitored?	Y	N	X	
161	Do you consider controlling how asset entry is recorded?	Y	N	X	
162	Do you consider controlling how assets exit your facilities?	Y	N	X	
163	Do you consider controlling how asset exit is authorized?	Y	N	X	
164	Do you consider controlling how asset exit is monitored?	Y	N	X	
165	Do you consider controlling how asset exit is recorded?	Y	N	X	
166	Do you consider formally managing the disposition of assets?	Y	N	X	
167	Do you consider sanitizing media prior to reuse, release, or disposal?	Y	N	X	
168	Do you consider formally controlling how your assets are sanitized?	Y	N	X	
169	Do you consider controlling how asset sanitizations are authorized?	Y	N	X	
170	Do you consider controlling how asset sanitizations are monitored?	Y	N	X	
171	Do you consider controlling how asset sanitizations are recorded?	Y	N	X	
PR.DS-4 ASSESS HOW WELL DATA AVAILABILITY IS BEING MANAGED					
172	Do you protect the availability of your data by maintaining adequate capacity?	Y	N	X	
173	Do you maintain data using methods that are consistent with your risk strategy?	Y	N	X	
174	Do you monitor data usage and carry out capacity planning for your systems?	Y	N	X	
175	Do you identify data capacity needs and requirements for each system?	Y	N	X	
176	Do you develop future capacity plans and projections for each system?	Y	N	X	
177	Do you establish redundant features if data availability cannot be guaranteed?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

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 a detailed set of audit questions (see above) and a general audit checklist (see pdf sample of our checklist).

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