Security Audit Program

ISO 28000 Supply Chain

Janco Associates, Inc.

2024

28000 Supply Chain Security Audit Program

		Comment	Yes	No	Weight	Negative Score	Positive Score
Security Risk Assessment and Planning		http://e-janco.com/Security.htm			**120**	**6**	**114**
Risk Assessment					120	**6**	**114**
1.01	Validate that your enterprise has a supply chain security policy in place				**40**		40
1.02	Validate that the policy provides clear direction for the supply chain security program.	*Not all procedures are documented*			**10**	1	9
1.03	Validate that the policy shows that your management is committed to supply chain security.				**10**		10
1.04	Validate that management supports the enterprise's supply chain security policy.				**10**		10
1.05	Validate that the policy shows that your management is prepared to support an ongoing commitment to supply chain security.	*Not all unit heads on on board*			**10**	2	8
1.06	Validate that the enterprise's supply chain security policy is consistent with your business objectives.				**10**		10
1.07	Validate that the enterprise's supply chain security policy meets the enterprise's business requirements.	*Not all commitments are signed*			**10**	1	9
1.08	Validate that the enterprise's supply chain security policy complies with all relevant laws and regulations.				**10**		10
1.09	Validate that Business Continuity and Disaster Recovery Plans address cyberattacks and Ransomware	*Documention not complete*			**10**	2	8

28000 Supply Chain Security Audit Program

	Weight	Negative Score	Positive Score
	2,169	168	2000
Security Risk Assessment and Planning	**120**	**6**	**114**
Risk Assessment	120	6	114
Supply Chain Security Management Objectives	**395**	**13**	**382**
Internal Security Organization	155	8	147
Implementation and Operation of Supply Chain Security	240	5	235
Organizational Supply Chain Security Management Objectives	**140**	**1**	**138**
Responsibility for the Supply Chain	70	0	69
Information Classification System	70	1	69
Human Resource Security Management Objectives	**185**	**131**	**54**
Security Prior to Employment	70	70	0
Security During Employment	60	60	0
Security at Termination	55	1	54
Physical and Environmental Supply Chain Security Management Objectives	**170**	**2**	**168**
Secure Areas	80	0	80
Enterprise Equipment	45	1	44
Remote Devices	45	1	44
Communications and Operations Management Objectives	**144**	**4**	**140**
Procedures and Responsibilities	10	0	10
Third Party Service Delivery	12	1	11
System Planning Activities	6	1	5
Malicious and Mobile Code	26	1	25
Back-up Procedures	6	0	6
Computer Networks	8	0	8
Media	30	0	30
Exchange of Information	18	0	18
Blockchain Interfaces	14	1	13
Information Processing Facilities	14	0	14
Information Access Control Management Objectives	**300**	**0**	**300**
Access to information	55	0	55
User Access Rights	25	0	25
Access Practices	50	0	50
Access to Network Services	40	0	40
Access to Operating Systems	45	0	45
Access to Applications	50	0	50
Mobile, and Remote Users	35	0	35
Systems Development and Maintenance Objectives	**327**	**11**	**316**
Information System Application Security	84	2	82
Applications Processing Information	91	7	84
Cryptographic Controls	60	2	58
System Files	50	0	50
Development and Support Processes.	42	0	42
Information Security Incident Management Objectives	**152**	**0**	**152**
Security Events and Weaknesses	88	0	88
Managing Security Incidents and Improvements	64	0	64
Disaster Recovery Plan and Business Continuity Objectives	**36**	**0**	**36**
Disaster Recovery Plan / Business Continuity	36	0	36
Compliance Management Objectives	**200**	**0**	**200**
Mandated Security Requirements	80	0	80
Security Compliance Reviews	70	0	70
Information System Audits	50	0	50

28000 Security Audit Program

	Weight	Negative Score	Positive Score
	2169	168	2000
Security Risk Assessment and Planning	120	6	114
Supply Chain Security Management Objectives	395	13	382
Organizational Supply Chain Security Management Objectives	140	1	138
Human Resource Security Management Objectives	185	131	54
Physical and Environmental Supply Chain Security Management Objectives	170	2	168
Communications and Operations Management Objectives	144	4	140
Information Access Control Management Objectives	300	0	300
Systems Development and Maintenance Objectives	327	11	316
Information Security Incident Management Objectives	152	0	152
Disaster Recovery Plan and Business Continuity Objectives	36	0	36
Compliance Management Objectives	200	0	200