Security Audit Program

Janco Associates, Inc.

2025

Table of Contents

Security Firewall Policy Checklist

Whether there are firewalls and a security policy or not, it's prudent to regularly evaluate your security approach. Review and answer the following questions before implementing any further firewall technology and/or security policy additions or changes.

Identify which resources must be secure and in which order of priority:

- Mission critical
- Redundant back-up system(s)
- Secondary
- Base systems

Identify minimum security needs for the following WAN connections:

- Employee remote access and dial-up
- Office-to-office VPN
- Employee and vendor bro
- Vendor access
- Business-to-business acce

Does the security team hav

- Network diagrams
- Trending data
- Protocol utilization
- Data points
- Access points
- Major vendors' point of contact information (ISP, telco, firewall vendor)

Does the security team know the order in which systems must be restored?

- The security response team must have a full understanding of which systems need to be restored to full operation and in what order.
- Does this order meet the business' objectives and priorities?

Does the information disclosure policy address the following about a security issue?

- What information is shared with others?
- Is information shared internally, departmentally, externally, etc?
- Under which circumstances?
- Mission critical information?
- Secondary intrusion information?
- Who has the authority to initiate information disclosure (Chief Security Officer, legal, HR)?

Ransomware, WFH, GDPR, CaCPA ISO, Cobit, HIPAA, and SOX Addressed

This audit program contains a list of tasks and and weights assigned to each task. The Excel sheet calculates the value of both positive and negative points. Based on the audit you place an "X" in the yes and/or no box and a value is automatically calculated. When the audit, which is on the worksheet 'Audit Program', is completed all of the results are them posted on the summary worksheet and graphic charts can be generated from those tables (see the attached sample).

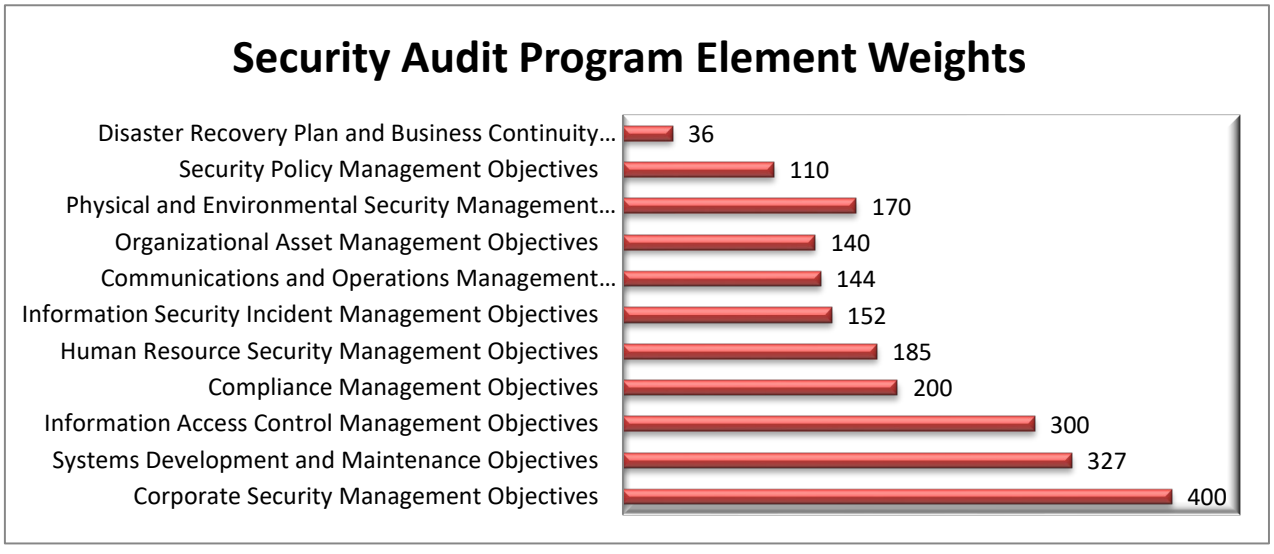
The worksheets Audit Program Summary, Audit Program, and Audit Program Graphic are integrated - if you change the name on the on any of those three worksheets then the Audit Program Summary Sheet and Audit Program Graphic will not be generated correctly. We suggest that you make a copy of the entire excel file and delete the "Sample" worksheets.

We have assigned weights to each element of the audit, you are free to updated to weights to what you think they should be. We assume no liability for the weight assignment and leave that up to the user. Our weights are only recommendations and should be considered as such.

The last three worksheets show a sample of the forms filled out with a set of summary graphic
We assume that the individual completi
Included with the excel spread sheet are
and used in the process. For ease you ca
excel worksheet.

NOTE: An item can be marked both as a
and negative score.

support@e-janco.com https://e-janco.com



Security Audit Program (Sample)

		Comment	Yes	No	Weight	Negative Score	Positive Score
Compliance Management Objectives					**200**	**0**	**200**
Mandated Security Requirements		https://www.e-janco.com/SarbanesOxley.htm			**80**	**0**	**80**
36.01	Validate that the enterprise's information systems comply with all relevant statutory security requirements.		x		10		10
36.02	Validate that the enterprise's information systems comply with all relevant regulatory security requirements.		x		10		10
36.03	Validate that the enterprise's information sy security requirements.		x		10		10
36.04	Validate the design the enterprise's informat statutory, regulatory, and contractual securi		x		10		10
36.05	Validate the operation of the enterprise's inf statutory, regulatory, and contractual securi		x		10		10
36.06	Validate the management of the enterprise's relevant statutory, regulatory, and contractu		x		10		10
36.07	Validate that the enterprise's users of the en relevant statutory, regulatory, and contractual security requirements.		x		10		10
36.08	Validate with legal experts in order to ensure that the enterprise's information systems comply with all relevant national and international legal security requirements.		x		10		10
Security Compliance Reviews					**70**	**0**	**70**
37.01	Validate that the enterprise's systems comply with the enterprise's security policies.		x		10		10
37.02	Validate that the enterprise's systems comply with the enterprise's security standards.		x		10		10
37.03	Validate the security of the enterprise's information systems.		x		10		10
37.04	Validate that the enterprise's information security reviews are carried out on a regular basis.		x		10		10
37.05	Validate the security of the enterprise's information systems by examining how well they comply with security policies.		x		10		10
37.06	Validate the technical platforms and information systems by examining how well they comply with relevant security implementation standards.		x		10		10
37.07	Validate the technical platforms and information systems by examining how well they comply with documented security control requirements.		x		10		10
Information System Audits					**50**	**0**	**50**
38.01	Validate performance audits are executed on the enterprise's information systems.		x		10		10
38.02	Validate controls to safeguard operational systems while information system audits are being performed are in place.		x		10		10
38.03	Establish controls to safeguard audit software and data files while information system audits are being performed.		x		10		10
38.04	Validate controls to safeguard the integrity of audit tools.		x		10		10
38.05	Validate controls to prevent the misuse of audit tools.		x		10		10

Security Sample Audit Program (Sample Results)

	Weight	Negative Score	Positive Score
Security Policy Management Objectives	110	10	110
Information Security Policy	110	10	110
Corporate Security Management Objectives	400	68	300
Internal Security Organization	160	38	90
External Use of the Enterprise Information	240	30	210
Organizational Asset Management Objectives	140	10	100
Responsibility for the Enterprise Assets	70	10	50
Information Classification System	70	0	50
Human Resource Security Management Objectives	185	40	145
Security Prior to Employment	70	20	50
Security During Employment	60	0	60
Security at Termination	55	20	35
Physical and Environmental Security Management Objectives	170	3	165
Secure Areas	80	0	80
Enterprise Equipment	45	0	45
BYOD Equipment -- Number Devices 75	45	3	40
Communications and Operations Management Objectives	144	30	112
Procedures and Responsibilities			8
Third Party Service Delivery			8
System Planning Activities			6
Malicious and Mobile Code			26
Back-up Procedures			6
Computer Networks			8
Media			28
Exchange of Information			0
Electronic Commerce	14	6	8
Information Processing Facilities	14	0	14
Information Access Control Management Objectives	300	40	260
Access to information	55	0	55
User Access Rights	25	0	25
Access Practices	50	0	50
Access to Network Services	40	40	0
Access to Operating Systems	45	0	45
Access to Applications	50	0	50
Mobile, Remote, and Work From Home	35	0	35
Systems Development and Maintenance Objectives	327	0	327
Information System Application Security	84	0	84
Applications Processing Information	91	0	91
Cryptographic Controls	60	0	60
System Files	50	0	50
Development and Support Processes.	42	0	42
Information Security Incident Management Objectives	152	88	64
Security Events and Weaknesses	88	88	0
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

Security Sample Audit Program Summary

	Weight	Negative Score	Positive Score
	2164	289	1819
Corporate Security Management Objectives	400	10	110
Systems Development and Maintenance Objectives	327	68	300
Information Access Control Management Objectives	300	10	100
Compliance Management Objectives	200	40	145
Human Resource Security Management Objectives	185	3	165
Information Security Incident Management Objectives	152	30	112
Communications and Operations Management Objectives	144	40	260
Organizational Asset Management Objectives	140	0	327
Physical and Environmental Security Management Objectives	170	88	64
Security Policy Management Objectives	110	0	36
Disaster Recovery Plan and Business Continuity Objectives	36	0	200