

Technical Review

Technical Risk Treatment Plan



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Table of Contents

01		Network Management Plan
02		Security Management Plan
03		Data Security Management Plan

Network Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
97	Upgrade or replace computers with operating systems that are no longer supported. <ul style="list-style-type: none"> <input type="checkbox"/> DESKPC-4PF2ICP / 176.16.1.177 / Windows 10 Pro Version 1909 <input type="checkbox"/> DESKPC-09UPSPO / fe80::62:b15d:dc6e:d08d%6,176.16.1.169 / Windows 10 Pro Version 1909 	H	H
90	Ensure anti-virus definitions are up to date on specified computers. <ul style="list-style-type: none"> <input type="checkbox"/> Computer: DESKPC-U1K3NAF IP Address: 176.16.1.175 Security Center: Windows Defender <input type="checkbox"/> Computer: DESKPC-4PF2ICP IP Address: 176.16.1.177 Security Center: Windows Defender 	H	H
90	Ensure anti-spyware definitions are up to date on specified computers. <ul style="list-style-type: none"> <input type="checkbox"/> Computer: DESKPC-U1K3NAF IP Address: 176.16.1.175 Security Center: Windows Defender <input type="checkbox"/> Computer: DESKPC-4PF2ICP IP Address: 176.16.1.177 Security Center: Windows Defender 	H	H
75	Address patching on computers missing 1-3 security patches. <ul style="list-style-type: none"> <input type="checkbox"/> APPSVR01 / fe80::4183:7729:9818:eb0f%5,176.16.1.14 / Windows Server 2016 Standard 	M	H





RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<input type="checkbox"/> DCTLR01 / fe80::6168:20a2:860a:bbe0%13,176.16.1.12 / Windows Server 2016 Standard <input type="checkbox"/> DESKPC-09UPSP0 / fe80::62:b15d:dc6e:d08d%6,176.16.1.169 / Windows 10 Pro Version 1909 <input type="checkbox"/> Mac Mini-CServ1 / 176.16.1.5 / Mac macOS 13.2.1 (22D68) <input type="checkbox"/> iMac Pro-Mktg1 / 176.16.1.15 / Mac macOS 10.15.7 (19H15)		





Medium Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
68	Free or add additional disk space for the specified drives. <input type="checkbox"/> DESKPC-U1K3NAF - C: : 0.03 GB free <input type="checkbox"/> DESKPC-4PF2ICP - C: : 0.01 GB free	H	L

Low Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
35	Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary. <input type="checkbox"/> abwfrcmbr / A Branaugh <input type="checkbox"/> ajwfrcmbr / A Jensen <input type="checkbox"/> aswfrcmbr / A Smith <input type="checkbox"/> Administrator / Administrator <input type="checkbox"/> dwfrcmbr / Dora Baxter <input type="checkbox"/> dkwfrcmbr / D Kindle <input type="checkbox"/> dwwfrcmbr / D White <input type="checkbox"/> jswfrcmbr / J Shearing <input type="checkbox"/> jwwfrcmbr / J Westerfield <input type="checkbox"/> lwwfrcmbr / L Wilson <input type="checkbox"/> mgwfrcmbr / M Green <input type="checkbox"/> mpwfrcmbr / M Peters <input type="checkbox"/> mwwfrcmbr / M Warly	L	M

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<ul style="list-style-type: none"> <input type="checkbox"/> pkwfrcmbr / P Kettering <input type="checkbox"/> pswfrcmbr / P Sulu <input type="checkbox"/> skwfrcmbr / S Kulynee <input type="checkbox"/> spwfrcmbr / S Photono <input type="checkbox"/> thwfrcmbr / T Harris <input type="checkbox"/> uwfrcmbr / unitbdr admin <input type="checkbox"/> wpwfrcmbr / W Paulson <input type="checkbox"/> ydwfrcmbr / Yami Dareloth <input type="checkbox"/> ylwfrcmbr / Y Leland 		
<p>30</p>	<p>Investigate all accounts with passwords set to never expire and configure them to expire regularly.</p> <ul style="list-style-type: none"> <input type="checkbox"/> MYCO.COM\aswfrcmbr / A Smith <input type="checkbox"/> MYCO.COM\dwfrcmbr / Dora Baxter <input type="checkbox"/> MYCO.COM\dkwfrcmbr / D Kindle <input type="checkbox"/> MYCO.COM\jswfrcmbr / J Shearing <input type="checkbox"/> MYCO.COM\jwwfrcmbr / J Westerfield <input type="checkbox"/> MYCO.COM\lwwfrcmbr / L Wilson <input type="checkbox"/> MYCO.COM\mgwfrcmbr / M Green <input type="checkbox"/> MYCO.COM\mpwfrcmbr / M Peters <input type="checkbox"/> MYCO.COM\pkwfrcmbr / P Kettering <input type="checkbox"/> MYCO.COM\spwfrcmbr / S Photono <input type="checkbox"/> MYCO.COM\thwfrcmbr / T Harris <input type="checkbox"/> MYCO.COM\ydwfrcmbr / Yami Dareloth <input type="checkbox"/> MYCO.COM\ylwfrcmbr / Y Leland <input type="checkbox"/> MYCO.COM\ajwfrcmbr / A Jensen <input type="checkbox"/> MYCO.COM\dwfrcmbr / D White <input type="checkbox"/> MYCO.COM\mtalman / M Talman <input type="checkbox"/> MYCO.COM\mwwfrcmbr / M Warly <input type="checkbox"/> MYCO.COM\pswfrcmbr / P Sulu <input type="checkbox"/> MYCO.COM\uwfrcmbr / unitbdr admin <input type="checkbox"/> MYCO.COM\wpwfrcmbr / W Paulson 		
<p>20</p>	<p>Upgrade computers that have operating systems in Extended Support before end of life.</p> <ul style="list-style-type: none"> <input type="checkbox"/> EXCHSVR01 / fe80::c48a:8133:22db:305f%14,fe80::dc13:a1e6:8745:9eb6%12,196.76.48.95,176.16.1.15 / Windows Server 2012 R2 Standard <input type="checkbox"/> SQLSVR01 / fe80::5072:f78c:9e73:a130%12,176.16.1.17 / Windows Server 2012 R2 Standard <input type="checkbox"/> DESKPC-RB3LBP3 / 		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	fe80::3196:5fc5:f131:a6b0%2,176.16.1.181 / Windows 10 Enterprise 2015 LTSB		
15	<p>Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on.</p> <ul style="list-style-type: none"> <input type="checkbox"/> WRKSTN7-2 / 176.16.1.115 / Windows 10 Pro Version 1909 <input type="checkbox"/> WRKSTN10-3 / 176.16.1.141 / Windows 10 Enterprise <input type="checkbox"/> WRKSTN8-1 / 176.16.1.128 / Windows 10 Pro Version 1909 <input type="checkbox"/> WS2012SVR / 176.16.1.135 / Windows Server 2012 Standard Evaluation <input type="checkbox"/> WRKSTN8-4 / 176.16.1.137 / Windows 10 Pro Version 1909 <input type="checkbox"/> WRKSTN7-1 / 176.16.1.126 / Windows 10 Professional 1909 <input type="checkbox"/> DESKPC-MJOD0L9 / 176.16.1.120 / Windows 10 Enterprise <input type="checkbox"/> DESKPC-MGMT01 / 176.16.1.113 / Windows 10 Enterprise <input type="checkbox"/> RFHVNDA1 / 176.16.1.11 / Windows Server 2016 Standard <input type="checkbox"/> WRKSTN8-3 / 176.16.1.136 / Windows 10 Pro Version 1909 <input type="checkbox"/> WRKSTN8-2 / 176.16.1.131 / Windows 10 Pro Version 1909 <input type="checkbox"/> BDR01 / 176.16.1.140 / Windows Server 2016 Standard 		
13	<p>Disable or remove user accounts for users that have not logged on to active directory in 30 days.</p> <ul style="list-style-type: none"> <input type="checkbox"/> ajwfrcmbr / A Jensen <input type="checkbox"/> arom / Axel Rom <input type="checkbox"/> Administrator / Administrator <input type="checkbox"/> dwwfrcmbr / D White <input type="checkbox"/> ebaldwin / Edward Baldwin <input type="checkbox"/> fowardslash / fowared slash <input type="checkbox"/> jknightling / Jorge Knightling <input type="checkbox"/> jasmus / Jeremy Asus <input type="checkbox"/> jgilligan / Julia Gilligan <input type="checkbox"/> jkalo / Jessica Kalo <input type="checkbox"/> jchestnut / Janet Chestnut 		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<input type="checkbox"/> jconway / Joseph Conway		
	<input type="checkbox"/> jdelaney / Jonah Delaney		
	<input type="checkbox"/> mwwfrcmbr / M Warly		
	<input type="checkbox"/> mjohnson / Maxwell Johnson		
	<input type="checkbox"/> mtalman / M Talman		
	<input type="checkbox"/> pwalker / Paula Walker		
	<input type="checkbox"/> pswfrcmbr / P Sulu		
	<input type="checkbox"/> sjane / Sonny Jane		
	<input type="checkbox"/> tshelman / Terri Shelman		
	<input type="checkbox"/> uwfrcmbr / unitbdr admin		
	<input type="checkbox"/> wpwfrcmbr / W Paulson		

Security Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
95	Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed. <ul style="list-style-type: none"> <input type="checkbox"/> Name: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) / CVSS: 7.5 / IP: 96.67.119.196 	H	H
77	Enable account lockout for all users.	H	H
75	Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed. <ul style="list-style-type: none"> <input type="checkbox"/> Name: SSL/TLS: Missing `secure` Cookie Attribute / CVSS: 6.4 / IP: 96.67.119.196 <input type="checkbox"/> Name: SSL/TLS: BREACH attack against HTTP compression / CVSS: 5.9 / IP: 96.67.119.196 <input type="checkbox"/> Name: SSL/TLS: Certificate Expired / CVSS: 5 / IP: 96.67.119.196 <input type="checkbox"/> Name: Missing `httpOnly` Cookie Attribute / CVSS: 5 / IP: 96.67.119.196 	H	H
72	Enable automatic screen lock on the specified computers. <ul style="list-style-type: none"> <input type="checkbox"/> APPSVR01 <input type="checkbox"/> DCTLR01 <input type="checkbox"/> DCTLR02 <input type="checkbox"/> EXCHSVR01 <input type="checkbox"/> FSSVR01 <input type="checkbox"/> HVSVR1 <input type="checkbox"/> SQLSVR01 	M	M

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

SQLSVR02

Data Security Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
87	<p>Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with PII should be investigated to see if a breach has occurred.</p> <ul style="list-style-type: none"> <input type="checkbox"/> msimpson : M Simpson <input type="checkbox"/> yslobedin : Y Slobedin 	H	H
87	<p>Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with ePHI should be investigated to see if a breach has occurred.</p> <ul style="list-style-type: none"> <input type="checkbox"/> pralston : P Ralston <input type="checkbox"/> jsmith : J Smith 	H	H
87	<p>Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with PCI Cardholder Data should be investigated to see if a breach has occurred.</p> <ul style="list-style-type: none"> <input type="checkbox"/> ahollings : A Hollings <input type="checkbox"/> srogers : S Rogers <input type="checkbox"/> ttrundle : T Trundle 	H	H
80	<p>Investigate the unauthorized computers storing GDPR Personal Data. Personal Data should be stored on computers in accordance with organization policy.</p> <ul style="list-style-type: none"> <input type="checkbox"/> WRKSTN10-4 / 176.16.1.133 	H	H

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
80	<p>Investigate the unauthorized computers storing ePHI. ePHI should be stored on computers in accordance with organization policy.</p> <ul style="list-style-type: none"> <input type="checkbox"/> DESKPC-35EGQCC / 176.16.1.79 <input type="checkbox"/> DESKPC-BDJFFLG / 176.16.1.63 <input type="checkbox"/> DESKPC-F6CKERQ / 176.16.1.59 	H_F	H_F
80	<p>Investigate the unauthorized computers storing PII. PII should be stored on computers in accordance with organization policy.</p> <ul style="list-style-type: none"> <input type="checkbox"/> DESKPC-35EGQCC / 176.16.1.79 <input type="checkbox"/> DESKPC-BDJFFLG / 176.16.1.63 <input type="checkbox"/> DESKPC-F6CKERQ / 176.16.1.59 <input type="checkbox"/> WRKSTN10-1 / 176.16.1.138 <input type="checkbox"/> WRKSTN10-4 / 176.16.1.133 	H_F	H_F
80	<p>Investigate the network shares authorized to store Sensitive Data with unrestricted access. Limit access to the minimum necessary.</p> <ul style="list-style-type: none"> <input type="checkbox"/> \\FSSVR01\Accounting : D:\Shares\Accounting <input type="checkbox"/> \\FSSVR01\Human Resources : D:\Shares\Human Resources <input type="checkbox"/> \\FSSVR01\Operations : D:\Shares\Operations 	H_F	H_F
78	<p>Ensure that data is properly backed up on computers with GDPR Personal Data. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed.</p> <ul style="list-style-type: none"> <input type="checkbox"/> WRKSTN10-4 / 176.16.1.133 	H_F	H_F
78	<p>Ensure that data is properly backed up on computers with PII. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed.</p> <ul style="list-style-type: none"> <input type="checkbox"/> DESKPC-35EGQCC / 176.16.1.79 <input type="checkbox"/> DESKPC-BDJFFLG / 176.16.1.63 <input type="checkbox"/> DESKPC-F6CKERQ / 176.16.1.59 	H_F	H_F

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<input type="checkbox"/> FSSVR01 / 176.16.1.161 <input type="checkbox"/> WRKSTN10-1 / 176.16.1.138 <input type="checkbox"/> WRKSTN10-4 / 176.16.1.133		
78	<p>Ensure that data is properly backed up on computers with ePHI. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed.</p> <input type="checkbox"/> DESKPC-35EGQCC / 176.16.1.79 <input type="checkbox"/> DESKPC-BDJFFLG / 176.16.1.63 <input type="checkbox"/> DESKPC-F6CKERQ / 176.16.1.59 <input type="checkbox"/> FSSVR01 / 176.16.1.161	H	H
75	<p>Implement disk encryption on computers storing ePHI.</p> <input type="checkbox"/> DESKPC-35EGQCC / 176.16.1.79 <input type="checkbox"/> DESKPC-BDJFFLG / 176.16.1.63 <input type="checkbox"/> DESKPC-F6CKERQ / 176.16.1.59 <input type="checkbox"/> FSSVR01 / 176.16.1.161	H	H
75	<p>Implement disk encryption on computers storing GDPR Personal Data.</p> <input type="checkbox"/> WRKSTN10-4 / 176.16.1.133	H	H
75	<p>Implement disk encryption on computers storing PII.</p> <input type="checkbox"/> DESKPC-35EGQCC / 176.16.1.79 <input type="checkbox"/> DESKPC-BDJFFLG / 176.16.1.63 <input type="checkbox"/> DESKPC-F6CKERQ / 176.16.1.59 <input type="checkbox"/> FSSVR01 / 176.16.1.161 <input type="checkbox"/> WRKSTN10-1 / 176.16.1.138 <input type="checkbox"/> WRKSTN10-4 / 176.16.1.133	H	H