Prioritized Remediation Guidance

Based on your residual risk and expected loss, the following prioritized controls would be the best course of action for reducing risk, improving maturity, and decreasing expected loss. The risk improvement and expected loss improvement assume that the recommended control was implemented at 85% or better.

Control Title	Control Description
13. Data Protection	Prevent data exfiltration, mitigate the effects of exfiltrated da..
20. Penetration Tests and Red Team Exercises	Test the overall strength of your defenses (the technology, the..
3. Secure Configuration for Hardware and So..	Establish, implement, and actively manage (track, report on, c..
9. Limitation and Control of Network Ports	Manage (track/control/correct) the ongoing operational use of..
4. Continuous Vulnerability Assessment and ..	Continuously acquire, assess, and take action on new informat..
6. Maintenance, Monitoring, and Analysis of ..	Collect, manage, and analyze audit logs of events that could he..
2. Inventory of Authorized and Unauthorized..	Actively manage (inventory, track, and correct) all software on..
16. Account Monitoring and Control	Actively manage the life cycle of system and application accou..
12. Boundary Defenses	Detect/prevent/correct the flow of information transferring n..
19. Incident Response and Management	In order to protect the organization's information, as well as it..
14. Controlled Access Based on the Need to ..	Track/control/prevent/correct secure access to critical assets (..
1. Inventory of Authorized and Unauthorized..	Actively manage (inventory, track, and correct) all hardware d..
7. Email and Web Browser Protections	Minimize the attack surface and the opportunities for attacker..
17. Security Skills Assessment and Appropri..	For all function roles, identify the specific knowledge, skills, an..
15. Wireless Access Control	Track/control/prevent/correct the security use of wireless loca..
5. Controlled Use of Administrative Privileges	Track/control/prevent/correct the use, assignment, and config..
11. Secure Configurations for Network Devic..	Establish, implement, and actively manage (track, report on, c..
18. Application Software Security	Manage the security life cycle of all in-house developed and ac..
8. Malware Defenses	Control the installation, spread, and execution of malicious co..
10. Data Recovery Capability	Back up critical information with a proven methodology for ti..