CYBER RAM

CRAM-CORA-FULL-03
25 December 2025

Cyber Operational Risk Assessment (CORA)

Quantitative and Mission Based Cyber Operational Risk Assessment

Prepared For:
Notional Dental Clinic

Prepared By:
Alec Buchanan
alec@cyber-ram.com

NOTICE: This is a notional assessment for a company named Notional Dental Clinic. All business information is notional, and not all information is included. In full and paid reports, all negotiated assessment information will be included.

Cyber Risk Summary

Average annualized cyber risk to the business across all mission areas

$69,009.45

Per Year

The overall cyber risk to Notional Dental Clinic is assessed as moderate, with a confidence level of 90% and an average variation of 10%. This assessment reflects both the current threat environment and the organization’s existing security posture.

Average Impact	Average Loss Event Frequency
$169,943.32	13.15 Years
Average impacts across mission areas	Average anticipated frequency of successful attacks

Findings Summary

Multiple findings indicate areas of high risk or high sensitivity within the organization’s operations. The probability of a vulnerability existing across the organization is high, and the likelihood of experiencing a threat event aligns with industry averages for both frequency and impact. Notably, while the organization has successfully separated mission area functions on its logical network, the storage of HIPAA-protected information on systems intended for non-clinical operations significantly increases risk—doubling exposure in this area.

Mission Area	Annualized Mission Risk	Risk Disbursement
Clinical Operations	$28,731.69	41%
Marketing	$759.56	1%
Scheduling & Resource Coordination	$16,073.53	24%
Financial Operations	$23,444.67	34%

Clinical Operations

Annualized cyber risk to the business for this mission area

$28,731.69

Per Year

Clinical operations are the core of Notional Dental Clinic’s mission, directly supporting patient care and treatment. Critical data in this area includes patient PII, EHRs, clinical credentials, and treatment plans. The loss or compromise of these assets would have immediate and significant consequences for patient safety, regulatory compliance, and business continuity.

Impact	Threat	Vulnerability
$258,551.50	9.8 Years	87%
Highest impact	Highest threat event frequency	Probability of vulnerability

	Confidentiality	Integrity	Availability
Impact	$258,551.50	$116,630.58	$116,630.58
Threat Frequency	8-9 years	7-8 years	7-8 years
Vulnerability Probability	87%	87%	87%
Total (Annualized Risk)	$28,731.69	$12,683.57	$12,683.57

Clinical Operations – Impacts

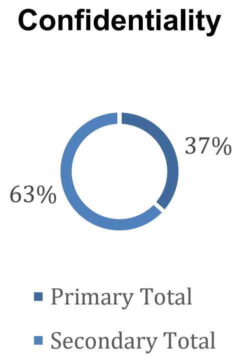
Highest cost for a loss event under this mission area

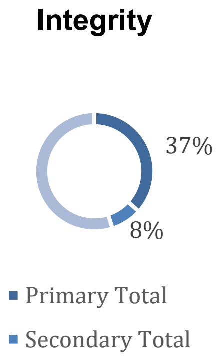
$258,551.50

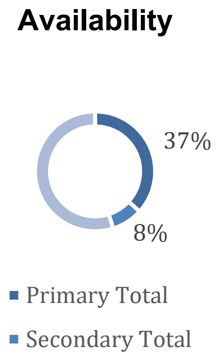
Per Loss Event

The results indicate that **loss of confidentiality presents the highest potential impact**, with a modeled event cost of approximately **$258,000**. This reflects the value of patient and business data, the likelihood of notification and restitution costs, and the longer-term effect of reputation and regulatory response. By comparison, incidents that primarily affect **data integrity or system availability** carry lower but still material impacts—around **$116,000 per event**—driven largely by downtime and recovery expenses.

Primary Impacts	**Confidentiality**	**Integrity**	**Availability**
Revenue Loss	$48,000.00	$48,000.00	$48,000.00
Productivity Loss	$28,800.00	$28,800.00	$28,800.00
Incident Response Costs	$8,100.00	$8,100.00	$8,100.00
Damage & Restoration	$10,000.00	$10,000.00	$10,000.00
Primary Total	$94,900.00	$94,900.00	$94,900.00
Secondary Impacts	**Confidentiality**	**Integrity**	**Availability**
Customer Restitution	$36,000.00	$4,428.00	$4,428.00
Reputational Damage (First Year)	$78,000.00	$14,820.00	$14,820.00
Regulatory & Legal	$49,651.50	$2,483.52	$2,483.52
Secondary Total	$163,651.50	$21,731.52	$21,731.52
Highest Impact			
			$258,551.50







Clinical Operations – Threats

Anticipated threat event frequency under this mission area

9.88

Years

Noticeable Threat Sources

Ransomware

Most Dangerous / Most Likely

Overview: Highly capable, organized cybercriminals that deploy encryption and data-theft campaigns to extort victims for financial gain. Their intent is profit-driven and persistent, targeting organizations with valuable or sensitive data to maximize ransom leverage.

Targets: PII, PHI, and assets/services/data critical to clinical operations

Data Broker

Overview: Moderately capable actors who collect, purchase, or steal large volumes of personal or corporate information for resale on dark-web markets. Their intent centers on monetizing data access rather than direct disruption, making them opportunistic but commercially motivated.

Targets: PII and PHI

Threat Summary

Expected frequency that a threat source will attempt to exploit and attack

Threat Source	Alignment (Intent)	Capability	TEF
Ransomware	100%	High	9.88 Years
Data Broker	100%	Moderate	11.2 Years
Botnet Operator	20%	Low	3 Years
Other (Nation State, Competitor, Insider, Terrorist, Hacktivist)	Negligible	Negligible	Negligible

Clinical Operations – Vulnerability

Estimated vulnerability existence probability (VEP) within this mission area

87%

VEP

18

Total Attack Surface

Critical Assets as Access Points

Impactful Privileges as Access Points

Vulnerability Existence Probability (VEP)						
Tactic	**Necessity**	**Governance Strength**	**Prevention Strength**	**Mitigation Strength**	**Recovery Strength**	**Strength Total**
Initial Access	100%	20%	50%	20%	80%	43%
Persistence	83%	20%	20%	20%	0%	13%
Privilege Escalation	78%	20%	20%	20%	0%	12%
Discovery	83%	20%	10%	20%	0%	10%
Defense Evasion	75%	20%	20%	20%	0%	11%
Credential Access	78%	20%	20%	20%	0%	12%
Lateral Movement	83%	20%	40%	20%	0%	17%
Collection	20%	20%	10%	20%	0%	3%
Command and Control	83%	20%	10%	20%	0%	10%
Exfiltration	20%	20%	10%	20%	0%	3%
Impacts	60%	20%	30%	20%	0%	11%
					Normalized VEP Total	**87%**

Page Intentionally Left Blank

Marketing

Annualized cyber risk to the business for this mission area

$759.56

Per Year

The Marketing mission area supports business growth and patient acquisition by managing public-facing communications, branding, and outreach activities. This mission area includes the creation, storage, and distribution of marketing materials, credentials used to access marketing platforms, and systems that support digital presence. While marketing operations do not typically process high volumes of sensitive data, disruption or manipulation of these functions can negatively impact credibility, customer trust, and revenue opportunities.

Impact	Threat	Vulnerability
$16,159.47	23 Years	92%
Highest impact	Highest threat event frequency	Probability of vulnerability

	Confidentiality	Integrity	Availability
Impact	$0.00	$16,159.47	$16,159.47
Threat Frequency	Negligible	20-26 years	20-26 years
Vulnerability Probability	92%	92%	92%
Total (Annualized Risk)	$0.00	$759.56	$759.56

Marketing – Impacts

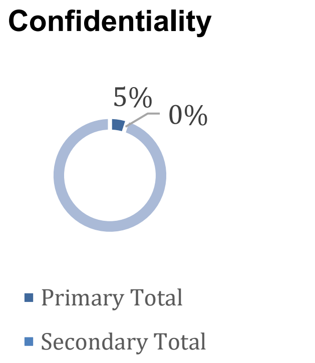
Highest cost for a loss event under this mission area

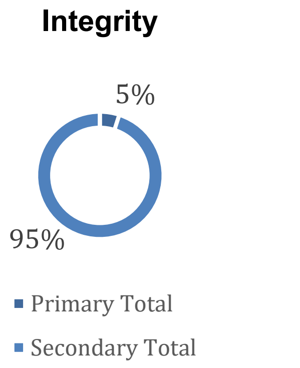
$16,159.47

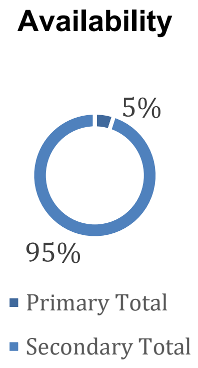
Per Loss Event

The results indicate that **loss of integrity and availability presents the highest potential impact**, with a modeled event cost of approximately **$16,000**. This reflects the value of credibility and opportunity. By comparison, incidents that primarily affect confidentiality carry lower—around **$800.00 per event**—due to the public nature of marketing materials and products.

Primary Impacts	**Confidentiality**	**Integrity**	**Availability**
Revenue Loss	$-	$-	$-
Productivity Loss	$400.00	$400.00	$400.00
Incident Response Costs	$-	$-	$-
Damage & Restoration	$400.00	$400.00	$400.00
Primary Total	$800.00	$800.00	$800.00
Secondary Impacts	**Confidentiality**	**Integrity**	**Availability**
Customer Restitution	$-	$-	$-
Reputational Damage (First Year)	$-	$-	$-
Regulatory & Legal	$-	$-	$-
Opportunity Cost	$-	$15,359.47	$15,359.47
Secondary Total	$-	$15,359.47	$15,359.47
Highest Impact			
			$16,159.47







Marketing – Threats

Anticipated threat event frequency under this mission area

23

Years

Noticeable Threat Sources

Cybercrime

Most Dangerous / Most Likely

Overview: Cybercriminals are individuals or organized groups using computers and networks for illegal activities like fraud, data theft, and spreading malware. Their primary motivations are often financial gain, but can also include political reasons, revenge, or the desire to cause disruption.

Targets: Credentials & Marketing Material

Insider

Overview: An insider threat involves current or former employees, contractors, or partners misusing legitimate access to an organization's assets. Damage can be intentional (theft, sabotage) or accidental (negligence). These threats bypass external security and pose significant risks to data integrity, primarily driven by motivations like financial gain, revenge, or human error.

Targets: Marketing Material

Threat Summary

Expected frequency that a threat source will attempt to exploit and attack

Threat Source	Alignment (Intent)	Capability	TEF
Cybercriminal	40%	High	23 Years
Insider	50%	Moderate	25 Years
Other (Nation State, Competitor, Insider, Terrorist, Hacktivist)	Negligible	Negligible	Negligible

Marketing – Vulnerability

Estimated vulnerability existence probability (VEP) within this mission area

92%

VEP

8

Total Attack Surface

Critical Assets as Access Points

Impactful Privileges as Access Points

Vulnerability Existence Probability (VEP)						
Tactic	**Necessity**	**Governance Strength**	**Prevention Strength**	**Mitigation Strength**	**Recovery Strength**	**Strength Total**
Initial Access	100%	20%	83%	0%	4%	27%
Persistence	0%	20%	100%	17%	4%	0%
Privilege Escalation	0%	20%	100%	17%	4%	0%
Discovery	100%	20%	33%	4%	4%	15%
Defense Evasion	50%	20%	58%	8%	4%	11%
Credential Access	100%	20%	33%	0%	4%	14%
Lateral Movement	0%	20%	100%	17%	4%	0%
Collection	100%	20%	0%	0%	0%	5%
Command and Control	0%	20%	100%	17%	4%	0%
Exfiltration	100%	20%	17%	0%	4%	10%
Impacts	0%	20%	100%	25%	4%	0%
					Normalized VEP Total	**92%**

Page Intentionally Left Blank

Scheduling & Resource Coordination

Annualized cyber risk to the business for this mission area

$16,073.53

Per Year

The Scheduling and Resource Coordination mission area supports the day-to-day operation of the clinic by managing patient appointments, staff availability, and allocation of clinical resources. This mission area enables efficient patient flow and directly affects revenue realization, productivity, and patient experience. Systems supporting scheduling often interface with clinical and financial functions, making their reliability and integrity critical to sustained operations.

Impact	Threat	Vulnerability
$172,365.94	9.33 Years	87%
Highest impact	Highest threat event frequency	Probability of vulnerability

	Confidentiality	Integrity	Availability
Impact	$78,422.40	$172,365.94	$172,365.94
Threat Frequency	12-16 years	8-10 years	8-10 years
Vulnerability Probability	87%	87%	87%
Total (Annualized Risk)	$4,873.39	$16,073.53	$16,073.53

Scheduling & Resource Coordination – Impacts

Highest cost for a loss event under this mission area

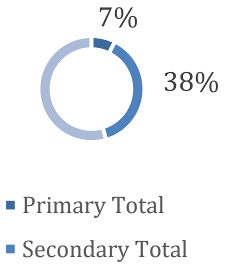
$172,365.94

Per Loss Event

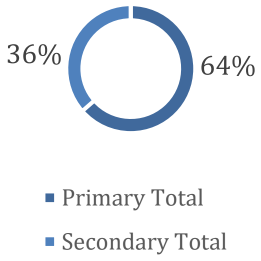
The results indicate that loss of integrity or availability presents the highest potential impact within the Scheduling and Resource Coordination mission area, with a modeled event cost of approximately **$172,000 per incident**. These impacts are driven by missed appointments, operational disruption, productivity loss, and downstream effects on revenue and patient experience. By comparison, loss of confidentiality carries a lower but still material impact—approximately **$78,000 per event**—reflecting limited data exposure, restitution requirements, and localized reputational effects.

Primary Impacts	**Confidentiality**	**Integrity**	**Availability**
Revenue Loss	$-	$96,955.13	$96,955.13
Productivity Loss	$400.00	$400.00	$400.00
Incident Response Costs	$9,000.00	$9,000.00	$9,000.00
Damage & Restoration	$3,200.00	$3,200.00	$3,200.00
Primary Total	$12,600.00	$109,555.13	$109,555.13
Secondary Impacts	**Confidentiality**	**Integrity**	**Availability**
Customer Restitution	$18,000.00	$-	$-
Reputational Damage (First Year)	$22,140.00	$22,140.00	$22,140.00
	$25,682.40	$25,311.34	$25,311.34
Regulatory & Legal	$-	$15,359.47	$15,359.47
Secondary Total	$65,822.40	$62,810.81	$62,810.81
Highest Impact			
			$172,365.94

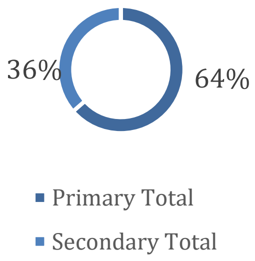
Confidentiality



Integrity



Availability



Scheduling & Resource Coordination – Threats

Anticipated threat event frequency under this mission area

9.88

Years

Noticeable Threat Sources

Ransomware

Most Dangerous / Most Likely

Overview: Highly capable, organized cybercriminals that deploy encryption and data-theft campaigns to extort victims for financial gain. Their intent is profit-driven and persistent, targeting organizations with valuable or sensitive data to maximize ransom leverage.

Targets: PII and assets/services/data critical to clinical operations

Data Broker

Overview: Moderately capable actors who collect, purchase, or steal large volumes of personal or corporate information for resale on dark-web markets. Their intent centers on monetizing data access rather than direct disruption, making them opportunistic but commercially motivated.

Targets: PII

Threat Summary

Expected frequency that a threat source will attempt to exploit and attack

Threat Source	Alignment (Intent)	Capability	TEF
Ransomware	100%	High	9.88 Years
Data Broker	100%	Moderate	11.2 Years
Botnet Operator	20%	Low	3 Years
Other (Nation State, Competitor, Insider, Terrorist, Hacktivist)	Negligible	Negligible	Negligible

Scheduling & Resource Coordination – Vulnerability

Estimated vulnerability existence probability (VEP) within this mission area

87%

VEP

18

Total Attack Surface

Critical Assets as Access Points

Impactful Privileges as Access Points

Vulnerability Existence Probability (VEP)						
Tactic	**Necessity**	**Governance Strength**	**Prevention Strength**	**Mitigation Strength**	**Recovery Strength**	**Strength Total**
Initial Access	100%	20%	50%	20%	80%	43%
Persistence	83%	20%	20%	20%	0%	13%
Privilege Escalation	78%	20%	20%	20%	0%	12%
Discovery	83%	20%	10%	20%	0%	10%
Defense Evasion	75%	20%	20%	20%	0%	11%
Credential Access	78%	20%	20%	20%	0%	12%
Lateral Movement	83%	20%	40%	20%	0%	17%
Collection	20%	20%	10%	20%	0%	3%
Command and Control	83%	20%	10%	20%	0%	10%
Exfiltration	20%	20%	10%	20%	0%	3%
Impacts	60%	20%	30%	20%	0%	11%
					Normalized VEP Total	**87%**

Page Intentionally Left Blank

Financial Operations

Annualized cyber risk to the business for this mission area

$23,444.67

Per Year

The Financial Operations mission area supports the clinic’s ability to collect revenue, manage payments, process insurance claims, and maintain accurate financial records. This mission area includes billing systems, payment processing platforms, financial data stores, and credentials used to access these systems. Financial Operations directly affect cash flow, regulatory compliance, and organizational trust, making this mission area highly sensitive to cyber events involving unauthorized access, manipulation, or disruption.

Impact	Threat	Vulnerability
$232,696.35	9.92 Years	94%
Highest impact	Highest threat event frequency	Probability of vulnerability

	Confidentiality	Integrity	Availability
Impact	$232,696.35	$172,365.94	$172,365.94
Threat Frequency	9-11 years	10-16 years	10-16 years
Vulnerability Probability	94%	94%	94%
Total (Annualized Risk)	$23,444.67	$13,258.92	$13,258.92

Financial Operations – Impacts

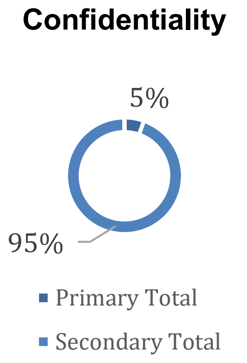
Highest cost for a loss event under this mission area

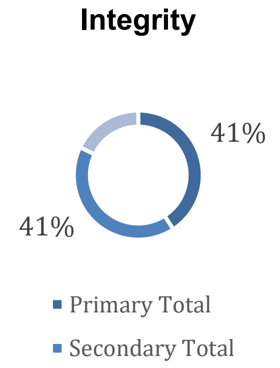
$232,696.35

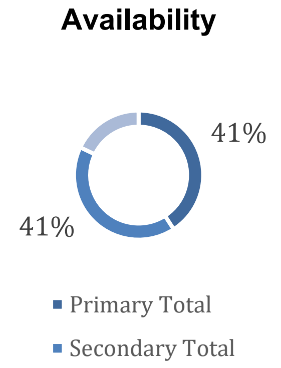
Per Loss Event

The results indicate that loss of confidentiality presents the highest potential impact within the Financial Operations mission area, with a modeled event cost of approximately **$232,000 per incident**. This reflects the exposure of financial and personal data, regulatory and legal consequences, customer restitution, and reputational damage. By comparison, incidents affecting data integrity or system availability carry slightly lower but still significant impacts—approximately **$190,000 per event**—driven by billing errors, delayed revenue collection, operational disruption, and recovery efforts.

Primary Impacts	**Confidentiality**	**Integrity**	**Availability**
Revenue Loss	$-	$52,884.62	$52,884.62
Productivity Loss	$400.00	$30,000.00	$30,000.00
Incident Response Costs	$9,000.00	$9,000.00	$9,000.00
Damage & Restoration	$3,200.00	$3,200.00	$3,200.00
Primary Total	$12,600.00	$95,084.62	$95,084.62
Secondary Impacts	**Confidentiality**	**Integrity**	**Availability**
Customer Restitution	$36,810.00	$-	$-
Reputational Damage (First Year)	$55,215.00	$55,215.00	$55,215.00
Regulatory & Legal	$128,098.80	$25,311.34	$25,311.34
Opportunity Cost	$-	$15,359.47	$15,359.47
Secondary Total	$220,123.80	$95,885.81	$95,885.81
Highest Impact			
			$232,696.35







Financial Operations – Threats

Anticipated threat event frequency under this mission area

9.92

Years

Noticeable Threat Sources

Ransomware

Most Likely / Most Dangerous

Overview: Highly capable, organized cybercriminals that deploy encryption and data-theft campaigns to extort victims for financial gain. Their intent is profit-driven and persistent, targeting organizations with valuable or sensitive data to maximize ransom leverage.

Targets: PII, PHI, and assets/services/data critical to clinical operations

Data Broker

Overview: Moderately capable actors who collect, purchase, or steal large volumes of personal or corporate information for resale on dark-web markets. Their intent centers on monetizing data access rather than direct disruption, making them opportunistic but commercially motivated.

Targets: PII and PHI

Threat Summary

Expected frequency that a threat source will attempt to exploit and attack

Threat Source	Alignment (Intent)	Capability	TEF
Ransomware	100%	High	9.92 Years
Data Broker	100%	Moderate	13.1 Years
Other (Nation State, Competitor, Insider, Terrorist, Hacktivist)	Negligible	Negligible	Negligible

Financial Operations – Vulnerability

Estimated vulnerability existence probability (VEP) within this mission area

94%

VEP

18

Total Attack Surface

Critical Assets as Access Points

Impactful Privileges as Access Points

Vulnerability Existence Probability (VEP)						
Tactic	**Necessity**	**Governance Strength**	**Prevention Strength**	**Mitigation Strength**	**Recovery Strength**	**Strength Total**
Initial Access	99%	20%	83%	0%	4%	27%
Persistence	0%	20%	99%	17%	4%	0%
Privilege Escalation	0%	20%	99%	17%	4%	0%
Discovery	99%	20%	33%	4%	4%	15%
Defense Evasion	50%	20%	58%	8%	4%	11%
Credential Access	99%	20%	33%	0%	4%	14%
Lateral Movement	0%	20%	99%	17%	4%	0%
Collection	99%	20%	0%	0%	0%	5%
Command and Control	0%	20%	99%	17%	4%	0%
Exfiltration	99%	20%	17%	0%	4%	10%
Impacts	0%	20%	99%	25%	4%	0%
					Normalized VEP Total	**94%**

Findings

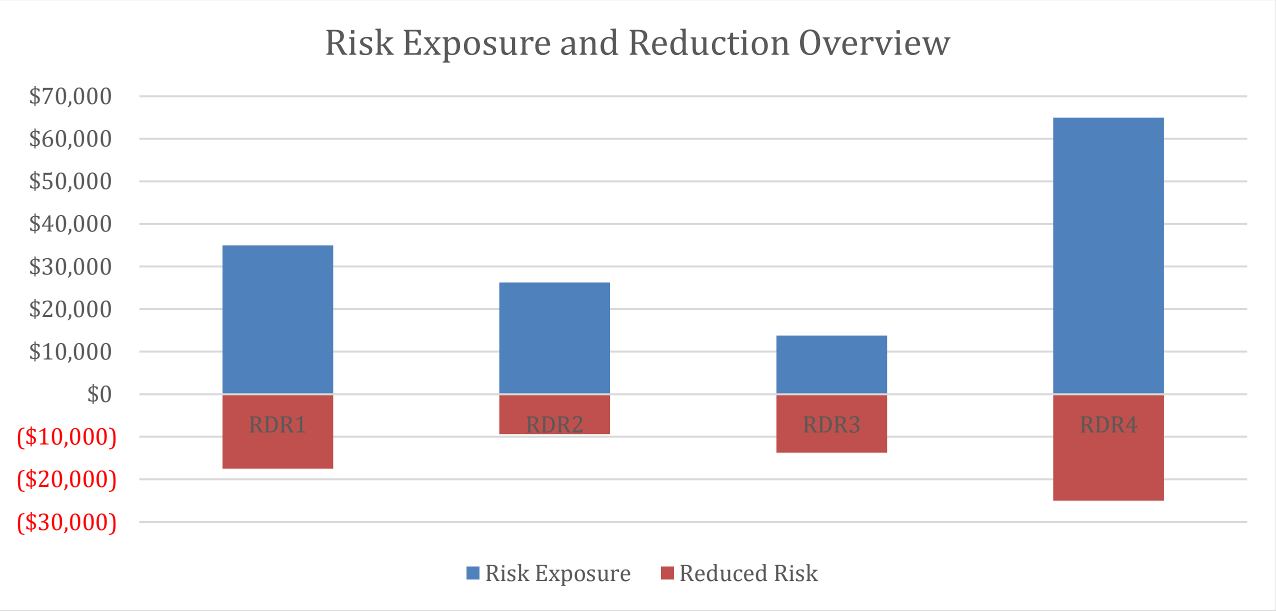
Future Testing

Areas of future testing include risk assessment components that either have high sensitivity, low confidence, or high variation. The intent of future testing is to turn assumptions into facts and create a more informed risk assessment.

PHI Distribution	Description: Determine if any untracked PHI, PII, or financial information is stored, processed, or transported by any unauthorized resources. Test Methodology: Enumerate all assets, services, and processes and search for PHI, PII, or financial information indicators.
Network Segmentation	Description: Determine the effectiveness of the separation between the administrative and clinical network. Additionally, identify specific capabilities required for lateral movement. Test Methodology: Evaluate the current controls and safeguards put in place to segment networks. Evaluate shared resources, trusted relationships, and the attack surface relative to each network.

Recommendations

Based on the risk analysis, the following actions are recommended to reduce the organization’s exposure to cyber threats, ensure the organization is operating within their identified and required risk appetite, and strengthen overall resilience. Each recommendation is supported by a Risk Detail Record (RDR) outlining the risk, proposed response, and estimated cost or resource requirements.



Risk Detail Record #1: Updates and Patching		
Risk Description	Continued use of Windows 10 workstations exposes the organization to vulnerabilities due to lack of ongoing security updates and support.	
Risk Category	Technical Vulnerability / Asset Management	
Current Risk Analysis		
Likelihood before controls: **0.2 Per Year**	Impact before controls: **$100,000 - $250,000**	Exposure Rating before controls: **$20,000 - $50,000**
Planned Risk Response	Select all that apply: □ Accept □ Avoid □ Transfer □ Mitigate	
Planned Risk Response Description	1. Upgrade all Windows 10 workstations to Windows 11 to ensure continued security patching and vendor support. This will reduce the risk of exploitation via known vulnerabilities. 2. Update current policy to prevent the use of non-supported systems.	
Planned Response Cost	$6,000–$8,000 (hardware/software upgrades, labor, and downtime)	
Notes	Prioritize clinical and administrative systems with access to sensitive data.	
Reduced Risk Analysis		
Likelihood after controls: **0.1 Per Year**	Impact after controls: **$100,000 - $250,000**	Exposure Rating after controls: **$10,000 - $25,000**

Risk Detail Record #2: Clinical Segmentation Enforcement		
Risk Description	HIPAA-protected information (e.g., patient release forms) is currently stored on the administrative network, increasing the risk of unauthorized access and regulatory non-compliance.	
Risk Category	Data Governance / Regulatory Compliance	
Current Risk Analysis		
Likelihood before controls: **0.15 Per Year**	Impact before controls: **$150,000 - $250,000**	Exposure Rating before controls: **$15,000 - $37,500**
Planned Risk Response	Select all that apply: □ Accept □ Avoid □ Transfer □ Mitigate	
Planned Risk Response Description	1. Identify and remove all HIPAA-regulated data from non-clinical networks. Restrict storage and processing such data to the clinical network only, with enforced access controls and monitoring. 2. Establish, communicate, and enforce policy for classifying data for easy identification. 3. Establish, communicate, and enforce policy for restricting the placement of HIPAA information on non-clinical networks.	
Planned Response Cost	$1,500–$4,000 (staff time, consulting, and network reconfiguration)	
Notes	Immediately focus on relocating patient release forms from the administrative network.	
Current Risk Analysis		
Likelihood after controls: **0.15 Per Year**	Impact after controls: **$75,000 - $150,000**	Exposure Rating after controls: **$11,250 - $22,500**

Risk Detail Record #3: Administrative Segmentation Establishment		
Risk Description	Customer WiFi is currently not segmented from the administrative network, increasing the risk of lateral movement by threat actors and potential exposure of sensitive systems.	
Risk Category	Network Architecture / Access Control	
Current Risk Analysis		
Likelihood before controls: **0.1 Per Year**	Impact before controls: **$75,000 - $200,000**	Exposure Rating before controls: **$7,500 - $20,000**
Planned Risk Response	Select all that apply: □ Accept □ Avoid □ Transfer □ Mitigate	
Planned Risk Response Description	1. Implement network segmentation to fully isolate customer WiFi from all internal administrative and clinical systems. Use VLANs or dedicated hardware to enforce separation.	
Planned Response Cost	$500–$2,000 (network hardware, configuration, and testing)	
Notes	Test segmentation to ensure no cross-network access is possible.	
Current Risk Analysis		
Likelihood after controls: **0 Per Year**	Impact after controls: **$75,000 - $200,000**	Exposure Rating after controls: **$0**

Risk Detail Record #4: Incident Response Planning		
Risk Description	The absence of a formal incident response plan increases mean time to recovery (MTTR) and may result in greater operational and financial impact during a cyber incident.	
Risk Category	Operational Resilience / Incident Management	
Current Risk Analysis		
Likelihood before controls: **0.5 Per Year**	Impact before controls: **$80,000 – $180,000**	Exposure Rating before controls: **$40,000 – $90,000**
Planned Risk Response	Select all that apply: ☐ Accept ☐ Avoid ☐ Transfer ☐ Mitigate	
Planned Risk Response Description	Develop and implement a comprehensive incident response plan, including defined roles, escalation procedures, and regular tabletop exercises. This will reduce MTTR and improve overall preparedness.	
Planned Response Cost	$6,000–$12,000 (staff training, consulting, plan development, and exercises)	
Notes	Review and update the plan annually or after any significant incident.	
Current Risk Analysis		
Likelihood after controls: **0.5 Per Year**	Impact after controls: **$40,000 - $120,000**	Exposure Rating after controls: **$20,000 - $60,000**

Appendix

A.1 Relevant Laws and Regulation

U.S.C Title 45

§ 164.308 Administrative safeguards:

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

§ 164.306 Security standards:

General rules.

(a) General requirements. Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protection.

A.2 Disclaimer

This Cyber Operational Risk Assessment (CORA) is based on information provided by the customer, publicly available data, industry trends, and analytical modeling techniques. The assessment relies on historical observations, probabilistic models, and reasonable assumptions to estimate potential impacts, likelihoods, and risk ranges.

While this assessment strives to achieve a confidence level of approximately 90%, cyber risk is inherently uncertain. Actual outcomes may differ materially due to changes in the threat environment, operational practices, system configurations, human behavior, or external factors beyond the control of Cyber RAM.

This report does not constitute a guarantee of security, compliance, or loss prevention. Implementation of recommendations may reduce risk but cannot eliminate it entirely. Cyber RAM shall not be held liable for losses, damages, or incidents resulting from the use of, reliance upon, or interpretation of this report.

This assessment is intended solely to support risk-informed decision-making and should be considered one input among others in the organization’s overall risk management and governance processes.

A.3 Process Overview

This report presents the results of a Cyber Operational Risk Assessment (CORA), a mission-based and quantitative approach to understanding cyber risk in business terms.

The assessment is structured to answer three key questions:

1. **What parts of the business matter most?**
   The organization’s mission is decomposed into mission areas that represent critical business functions. Each mission area is evaluated independently to determine how cyber incidents would affect operations, revenue, compliance, and reputation.

2. **How could those mission areas fail?**
   For each mission area, potential failures are evaluated across confidentiality, integrity, and availability. These failure modes represent the fundamental ways in which cyber events can disrupt business operations.

3. **What is the expected impact and likelihood?**
   Impacts are quantified in financial terms, while threat frequency and vulnerability conditions are modeled to estimate annualized cyber risk. Results are expressed as ranges to reflect uncertainty and variability.

The report is intended to be used as a decision-support tool. Leadership can use the findings to:

- Prioritize risk reduction efforts
- Evaluate the cost-effectiveness of security investments
- Make informed risk acceptance or mitigation decisions
- Support compliance and audit readiness

Recommendations are provided with estimated costs and expected risk reduction to help align cybersecurity actions with business objectives and risk tolerance.