ESTRATEGIA DE CIBERSEGURIDAD PARA ACTUALIZACIÓN TECNOLÓGICA DE PORTAL DE EMPACADORES (PAQPRO)

Aguacatitos Mercantil del Norte A.C.

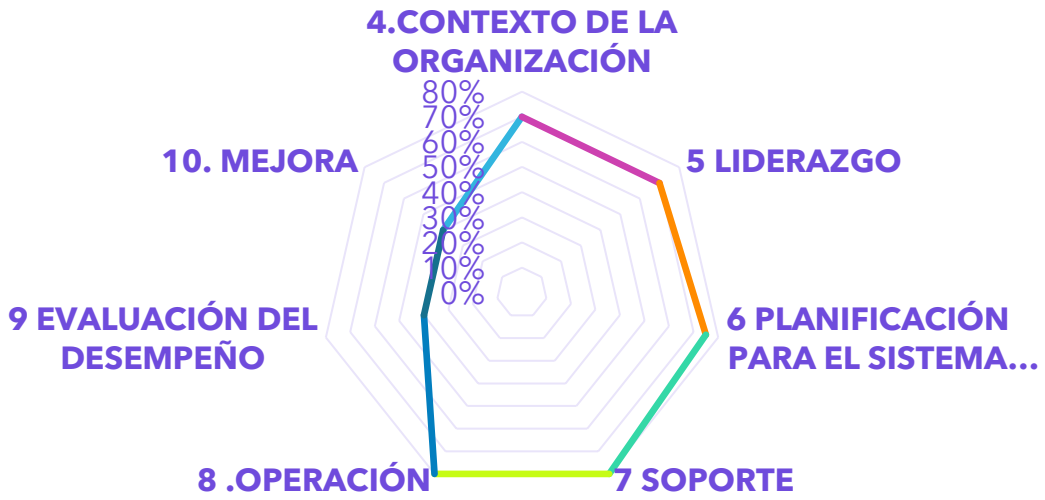
04 de Agosto 2024

AGENDA

1. Contexto Organizacional
2. Key Drivers
3. Situación de la empresa
4. Estrategia
5. Recursos necesarios
6. Plan de Trabajo 2024-2025

Contexto Organizacional

GAP ANALYSIS ISO 27001

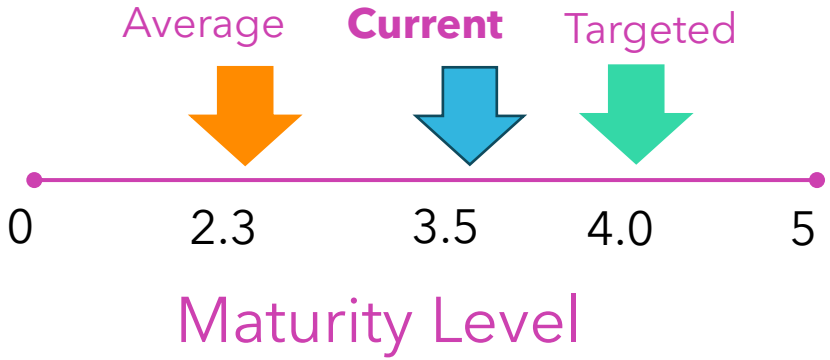


4.CONTEXTO DE LA ORGANIZACIÓN	70%
5 LIDERAZGO	70%
6 PLANIFICACIÓN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD	75%
7 SOPORTE	80%
8 .OPERACIÓN	80%
9 EVALUACIÓN DEL DESEMPEÑO	40%
10. MEJORA	40%
% de implementación SGSI	68%

% de implementación SGSI	Nivel de madurez
0%-20%	1
21%-40%	2
41%-60%	3
61%-80%	4
81%-100%	5

S.M.A.R.T Cybersecurity Maturity Gap Analysis Table

- **Current Maturity Level**: 3.2
- **Target Maturity Level**: 4.0
- **Gap**: The difference between the current and target maturity levels.
- **Relevant**: Goals aligned with overall cybersecurity strategy.
- **Time-bound**: Time frame for achieving the goals (18 months).

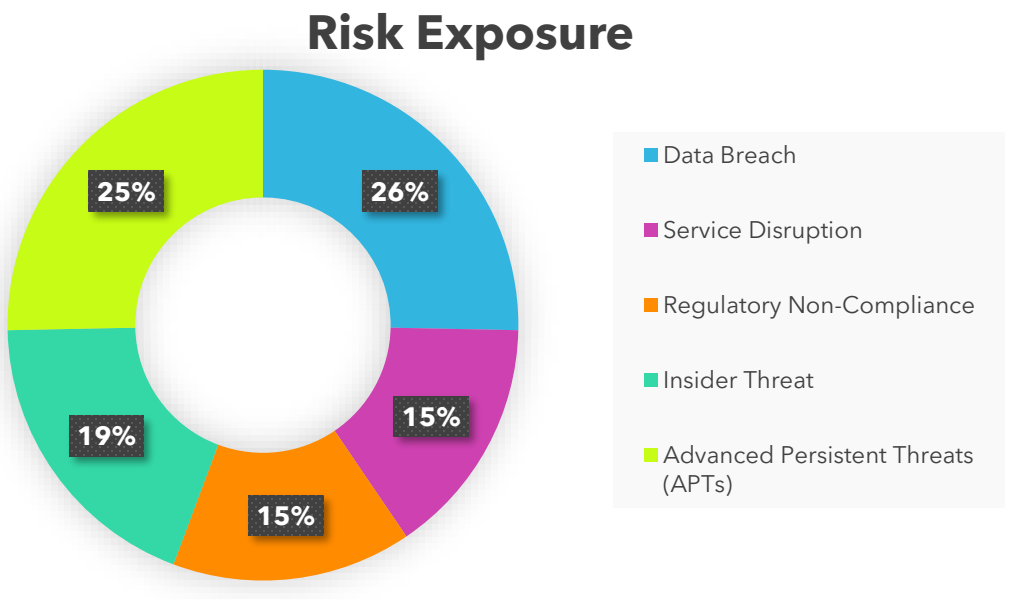


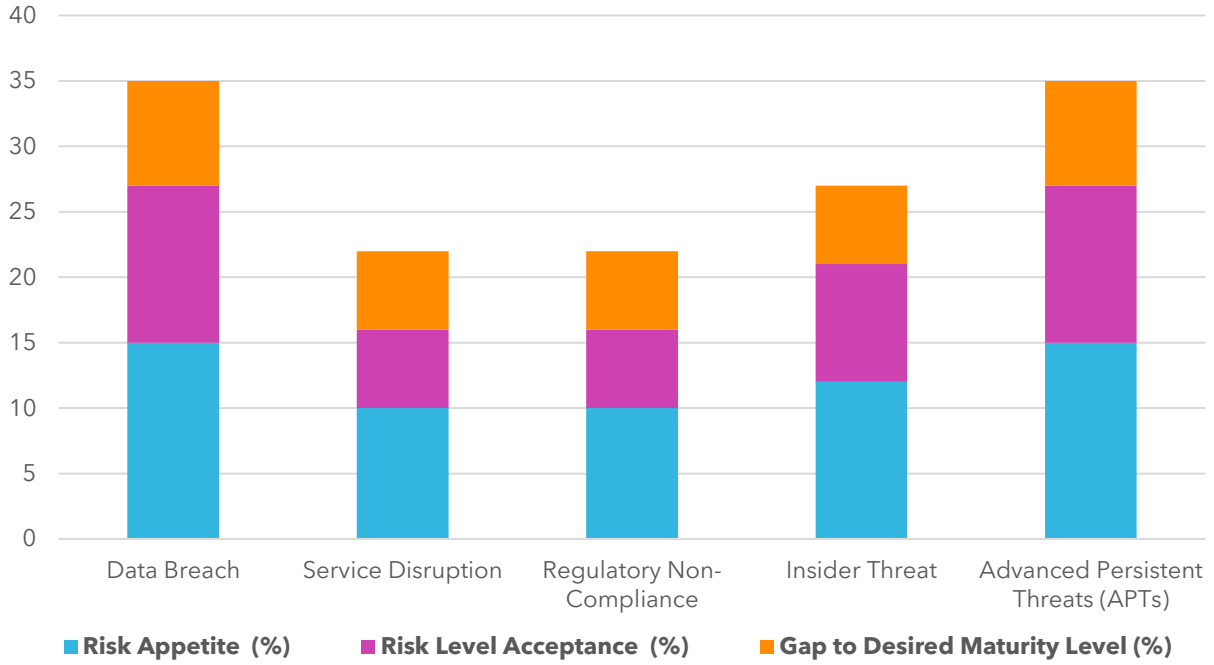
Key Drivers

		NEGOCIO		
Brand Engagement	**Adquisition**	**Holdbacking**	**Value**	**Loyalty**
• Campañas de fidelización • Eventos • Publicidad y marketing	• Partners reclutation • Channels developtment • Inside sales	• Asistencia a la Producción Proceso de Transporte	• Creación de Paquetes • Fumigación y • Recursos agrarios	• Partner Program • Channel Point Program
		TECNOLOGÍA		
Operation	**Ops Support**	**Bussiness Support**	**Customers**	**Users**
		• PAQPRO Web Application		

Situación de la Empresa

Bussiness Process Risk Assesment Updated





Risk Appetite: This is the percentage of risk the organization is willing to tolerate. 15%
Risk Level Acceptance: This represents the maximum acceptable risk percentage based on the target maturity level.
Desired Risk Level Acceptance:12%
Gap to Desired Maturity Level: This is the difference between the current risk exposure and the desired risk level acceptance.

Gap= Current Risk Exposure − Desired Risk Level Acceptance

Gap = 20%−12%=8%

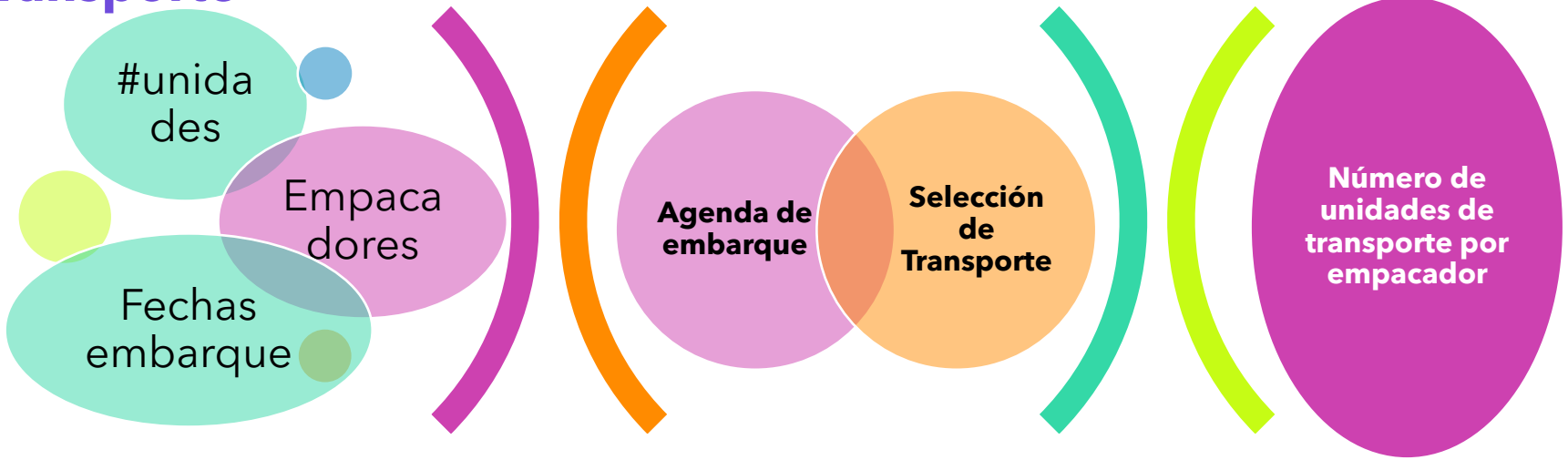
Riesgo General Actual

Riesgo Proceso Negocio

Situación de la empresa

Proceso de Transporte

Stakeholders
Dueño PAQPRO
Dueño Proceso Transporte
COO
VP Tecnología



Stakeholders
Productores
Empacadores

20%

Riesgo Proceso de Empaquetado

35%

Riesgo Aplicación PAQPRO (2024)

12%

Riesgo Objetivo del Proceso (2025)

SITUACIÓN ACTUAL:

La retención de nuevos empacadores ha caído un 15% en el último año debido a una falla de lógica en la aplicación web CORE que soporta este proceso (PAQPRO).

PAQPRO carece de un Identity Autentication Management Control que impida que los empacadores programen robots que puedan producer una comptencia desleal y monopolización del transporte de **Aguacatitos Mercantil del Norte AC.**

Si la retención continua cayendo, la entidad regulatoria nacional de Transportistas considerará esto como un caso de monopolización, acreedor a una multa mayor al costo del despliegue de la presente estrategia.

Estrategia de Ciberseguridad Asociada

Visión Estratégica

Actualización tecnológica de la FUNCIONALIDAD ÚNICA de autenticación actual para incluir funciones de manejo de identidades, controles de comportamiento humano (captcha), factores de autenticación biométricos y controles contra el robo de solicitudes, atendiendo el enfoque de defensa en profundidad utilizado para el resto de los sistemas administrados en conjunto por Tecnologías de la información y el departamento de seguridad.

La actualización será llevada a cabo desarrollando un módulo independiente que se integrará dentro del flujo de la aplicación actual lo que operativamente permitirá que dicha actualización se realice sin pérdida de la disponibilidad y permitirá realizar la integración de nuevos proveedores de desarrollo. Está prevista para ejecutarse en 12 meses

Priorización			Drivers	
Disponibilidad	Integridad	Cumplimiento	HOLDBACKING	BUSSINESS SUPPORT
El sistema actual nunca dejará de Operar hasta su ventana de actualización reemplazo	El módulo no almacena ni almacenará información por lo que ningún dato será susceptible a corrupción.	El tiempo planificado es menor al solicitado ante la comisión reguladora para corrección del problema	**Stakeholders asociados** FINANCIERO	OPERATIVO HUMANO

Estrategia de Ciberseguridad Asociada

Visión Estratégica

- Construcción de la aplicación
- Integración del enfoque de defensa en profundidad
- Pruebas metodología ágil

- Codificación módulo
- Integración autenticación
- Integración IAM
- Integración Biométricos
- Integración Captcha

Elección de proveedores, evaluación y ejecución de plan de actividades basado en el proceso de Operaciones de Seguridad del SGSI Actual

- Pruebas módulo
- Pruebas UAT (negocio)
- Capacitación Empacadores
- Pruebas con empacadores
- Ventana de mantenimiento
  - Evaluación de controles (Update SoA)
  - Planeación de los Request for Change (RFC) con aprobación del CAB/seguridad
  - Evaluación Seguridad de proveedores de acuerdo a ISO27002
  - Actualizar Documentación procesos de seguridad
- Monitoreo proceso transporte
- Modo aprendizaje del sistema.
- Ajustes

Recursos Necesarios

Financieros

- 10 MDP desarrollo
- 3 MDP QA
- 2 MDP Seguridad
- 2 MDP Riesgo Operativo

Operativos

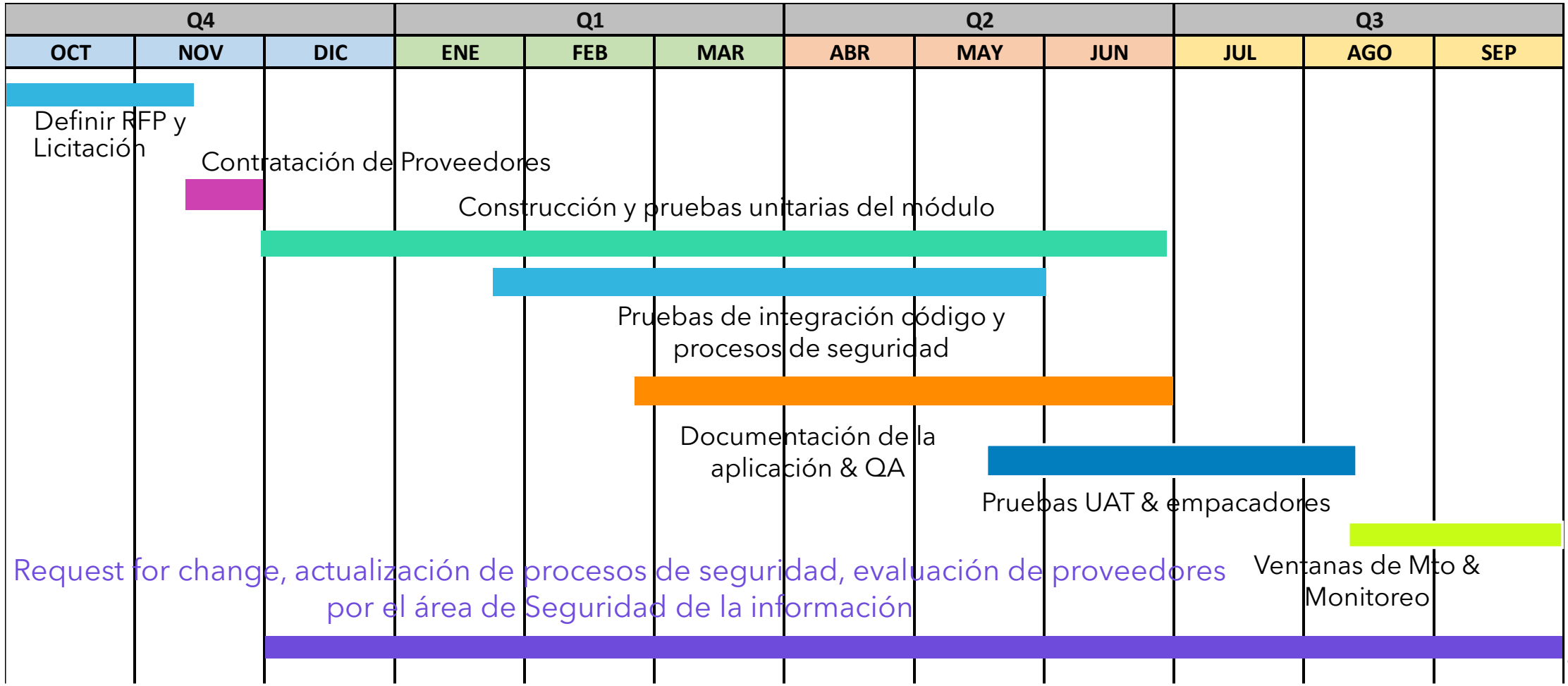
- Proveedor de desarrollo
- Proveedor pruebas
- Proveedor seguridad
- PM por parte de cada proveedor.
- Recursos operativos dedicados por parte de cada proveedor

Humanos

- PM dedicado
- Integrante del equipo de seguridad full Time
- Integrante del equipo de tecnologías de la información full Time
- Stakeholders asignación parcial:
  - Dueño del activo
  - Dueño de proceso
  - Representante Empacadores

PLAN DE TRABAJO

Roadmap Estrategia 2024-2025



LAMINAS DE APOYO PARA DUDAS

NIST CSF Function	Current Maturity Level (3.2)	Target Maturity Level (4.0)	Gap	Specific Goals	Measurable Metrics	Achievable Actions	Relevant Improvements
Identify	3.2	4.0	**0.8**	Enhance asset management; Improve risk assessment processes.	Implement advanced asset management tools; Conduct comprehensive risk assessments.	Invest in asset management solutions; Train staff on risk assessment.	Improved asset visibility; Better risk management.
Protect	3.2	4.0	**0.8**	Implement advanced security controls; Standardize protection measures.	Deploy next-gen firewalls; Establish uniform security policies.	Upgrade security infrastructure; Develop standardized policies.	Stronger protection against threats; Consistent security practices.
Detect	3.2	4.0	**0.8**	Deploy advanced detection tools; Improve threat monitoring.	Integrate SIEM solutions; Enhance real-time monitoring capabilities.	Purchase and configure SIEM; Increase monitoring coverage.	Faster detection of threats; Improved incident response.
Respond	3.2	4.0	**0.8**	Develop comprehensive incident response plans; Conduct regular drills.	Create detailed response plans; Schedule and perform incident response exercises.	Develop response documentation; Organize training sessions.	Better preparedness for incidents; Reduced response times.
Recover	3.2	4.0	**0.8**	Strengthen recovery plans; Test and update recovery strategies.	Implement robust backup solutions; Regularly test recovery procedures.	Invest in backup solutions; Perform regular recovery tests.	Enhanced recovery capability; Reduced downtime.

Gap Analysis

AguacateraMercantil del Norte AC

S.M.A.R.T Cybersecurity Maturity Gap Analysis Table Definitions:

- **Current Maturity Level**: 3.2
- **Target Maturity Level**: 4.0
- **Gap**: The difference between the current and target maturity levels.
- **Specific**: Clearly defined improvement goals.
- **Measurable**: Quantitative metrics for measuring progress.
- **Achievable**: Realistic improvement targets based on resources.
- **Relevant**: Goals aligned with overall cybersecurity strategy.
- **Time-bound**: Time frame for achieving the goals (18 months).

Risk Category	Current Risk Level	Target Risk Level	Key Risks	Mitigation Strategies	Current Risk Score	Target Risk Score
Supply Chain Risks	Medium	Low	Dependency on third-party vendors and insufficient visibility.	Implement comprehensive third-party risk assessments and continuous monitoring.	55	30
Data Breach Risks	High	Medium	Sensitive data exposure and potential unauthorized access.	Enhance encryption protocols, implement data loss prevention tools, and conduct regular audits.	70	45
Insider Threats	Medium	Low	Lack of employee training and awareness on security protocols.	Develop ongoing training programs and enforce strict access controls and monitoring.	60	35
Compliance Risks	Low	Low	Non-compliance with evolving regulations and standards.	Regularly update compliance frameworks and conduct audits to ensure adherence.	40	20
Technology Risks	Medium	Low	Outdated systems and insufficient patch management.	Upgrade legacy systems, enforce regular patching, and deploy endpoint protection solutions.	65	30
Reputation Risks	Medium	Low	Potential negative impact due to cybersecurity incidents.	Develop a crisis communication plan and enhance public relations strategies.	60	35

Risk assessment detailed