

# IT Risk Management at High Gear Engines



# Meet the team



**Shane Rodriguez**



**Garrett Williams**



**Jong Won Choi**



**Anirban Das**

# Agenda

 Introduction

 Financials

 Recommendation

 Risks and Mitigation

 Implementation

 Conclusion

# How can HG analyze and mitigate “quick win” IT risks and structure processes for future mitigation?

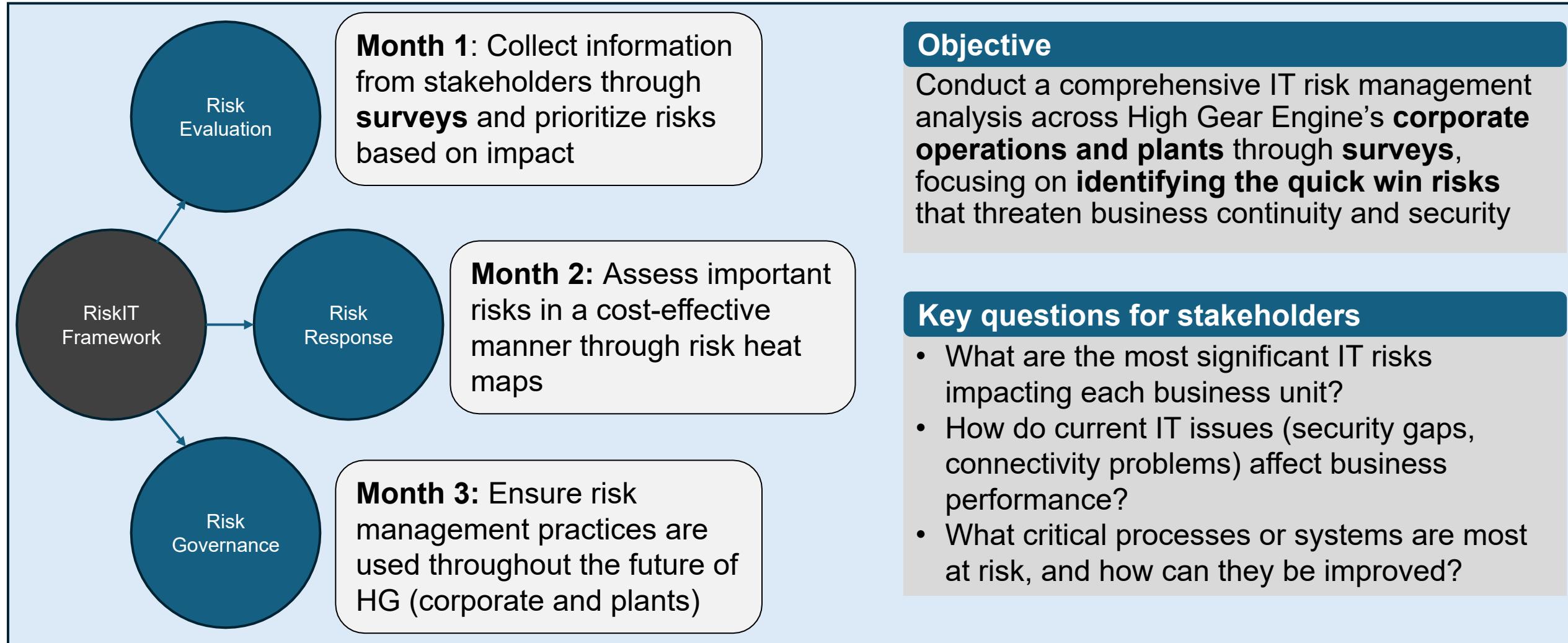


High Gear Engine Company (HG) is a global automotive supplier that has experienced significant growth in recent years. Following a near-bankruptcy during the 2008 financial crisis, HG has made a strong recovery and is now positioned for expansion

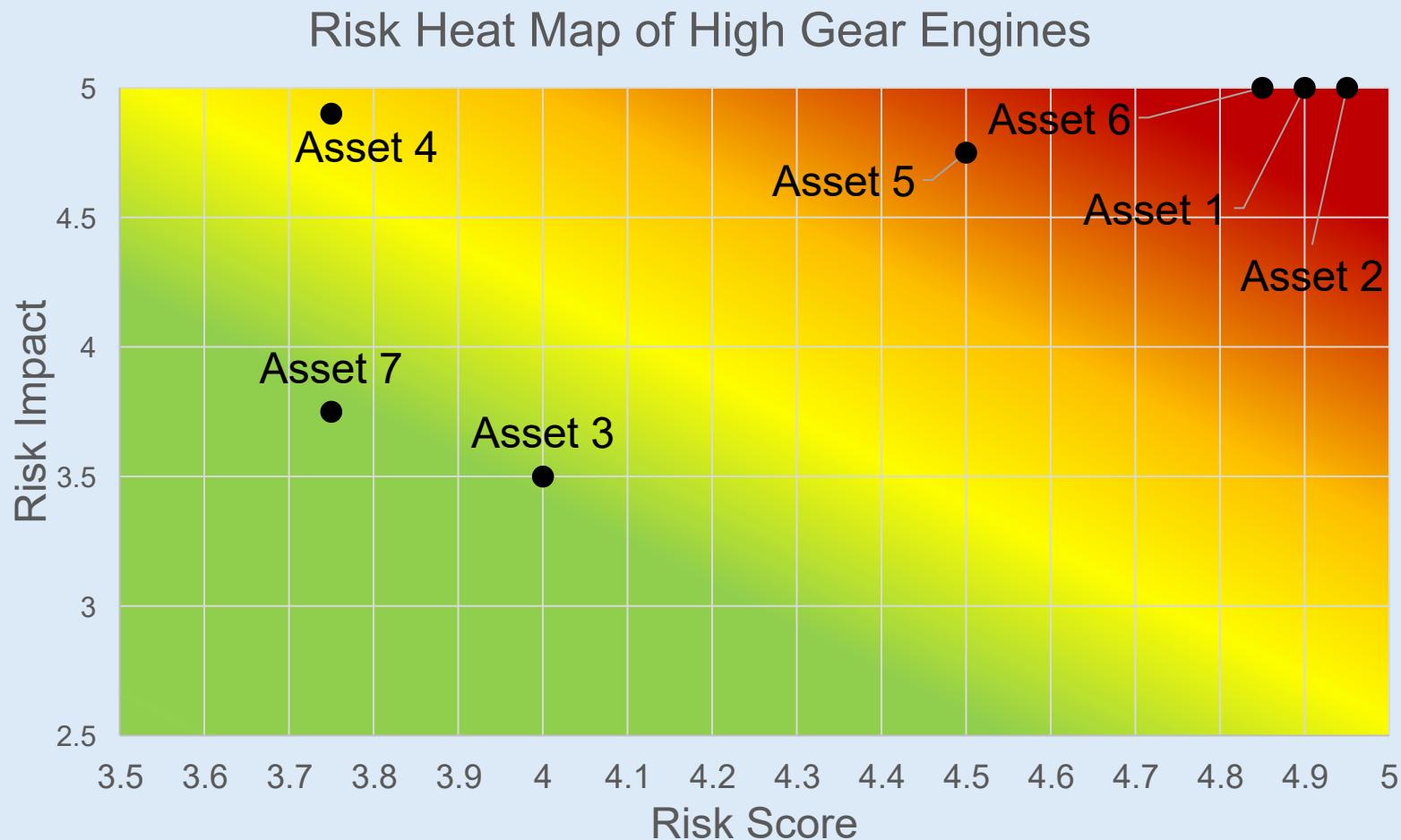


The outdated systems are causing costly production outages, poor network connection leads to slow work, and there's no formal IT risk management or security leadership, putting the company at significant operational risk

# Conducting a risk assessment over the next 3 months with RiskIT framework

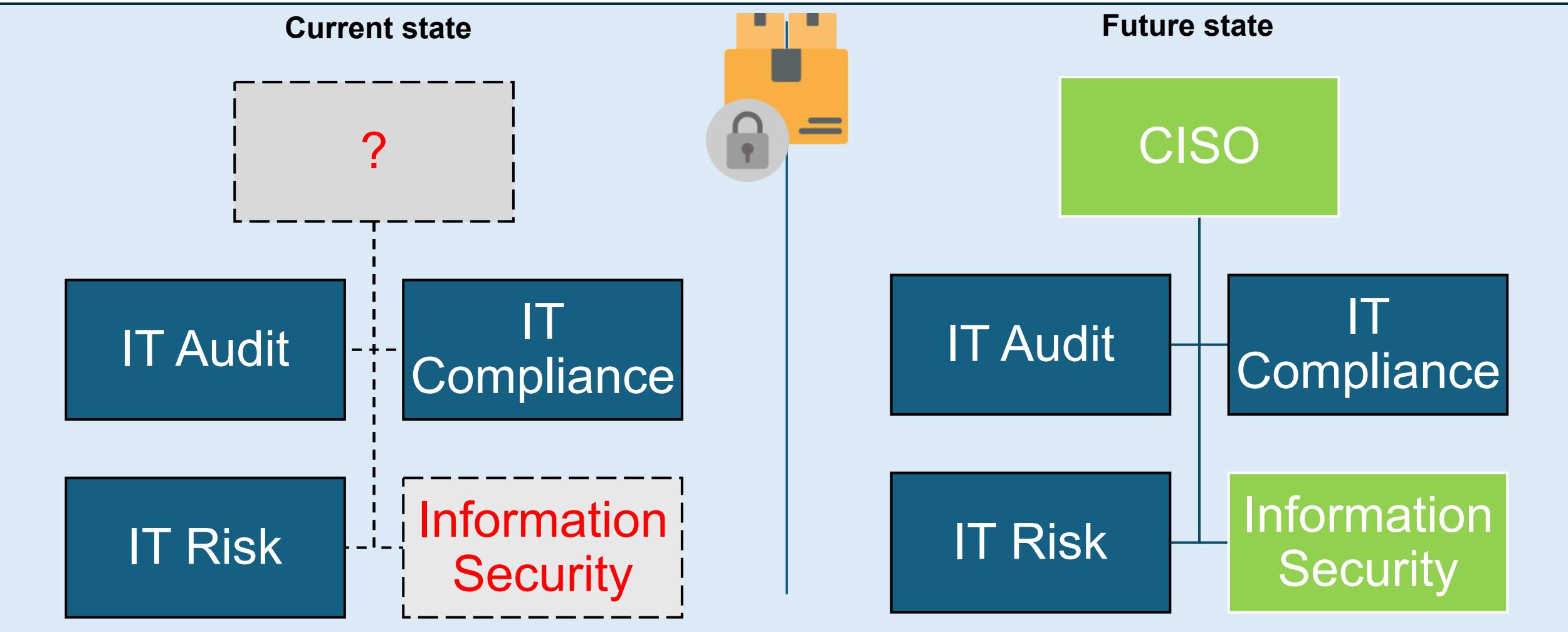


# Uncovering opportunities with strategic risk assessment tools

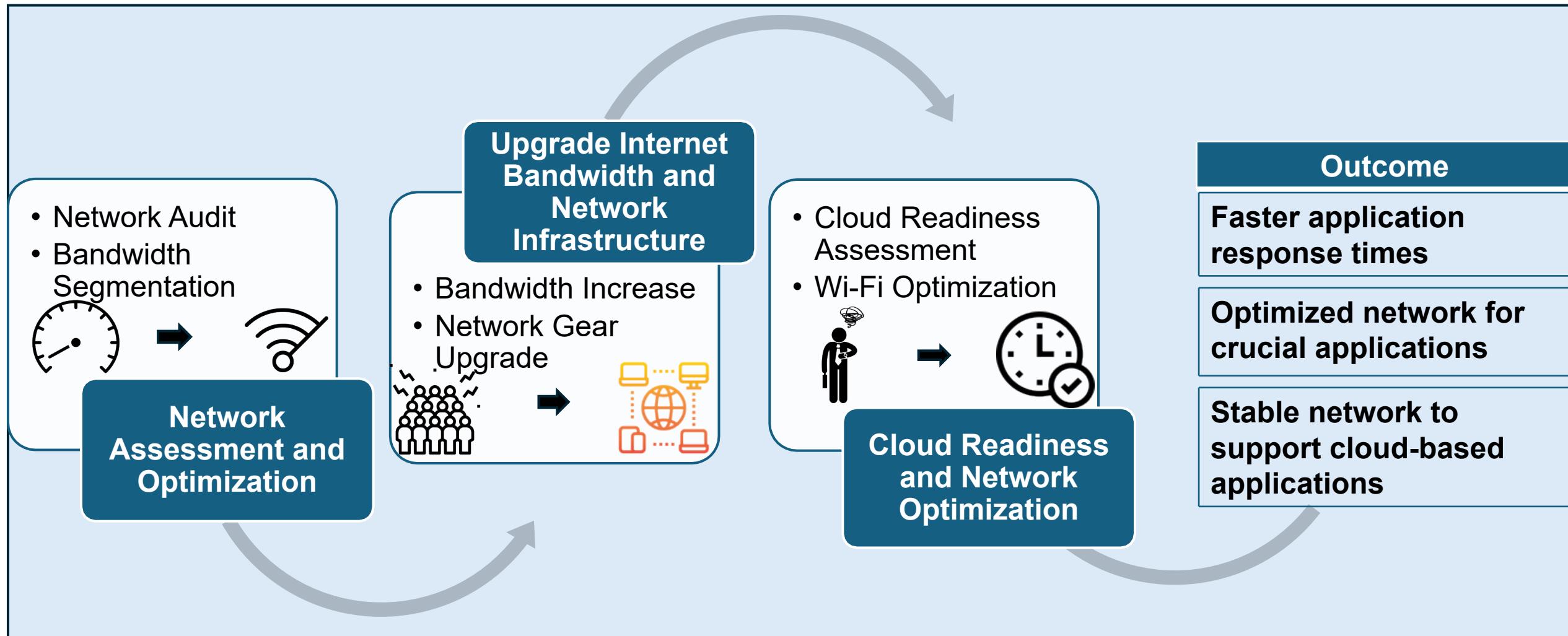


Identifier	Risk Description
Asset 1	Lack of accountability in security
Asset 2	Connectivity issues
Asset 3	Fragmented ERP systems
Asset 4	Unaddressed audit issues
Asset 5	Shop floor systems failures
Asset 6	Legacy software and hardware vulnerabilities
Asset 7	Over-reliance on vendors

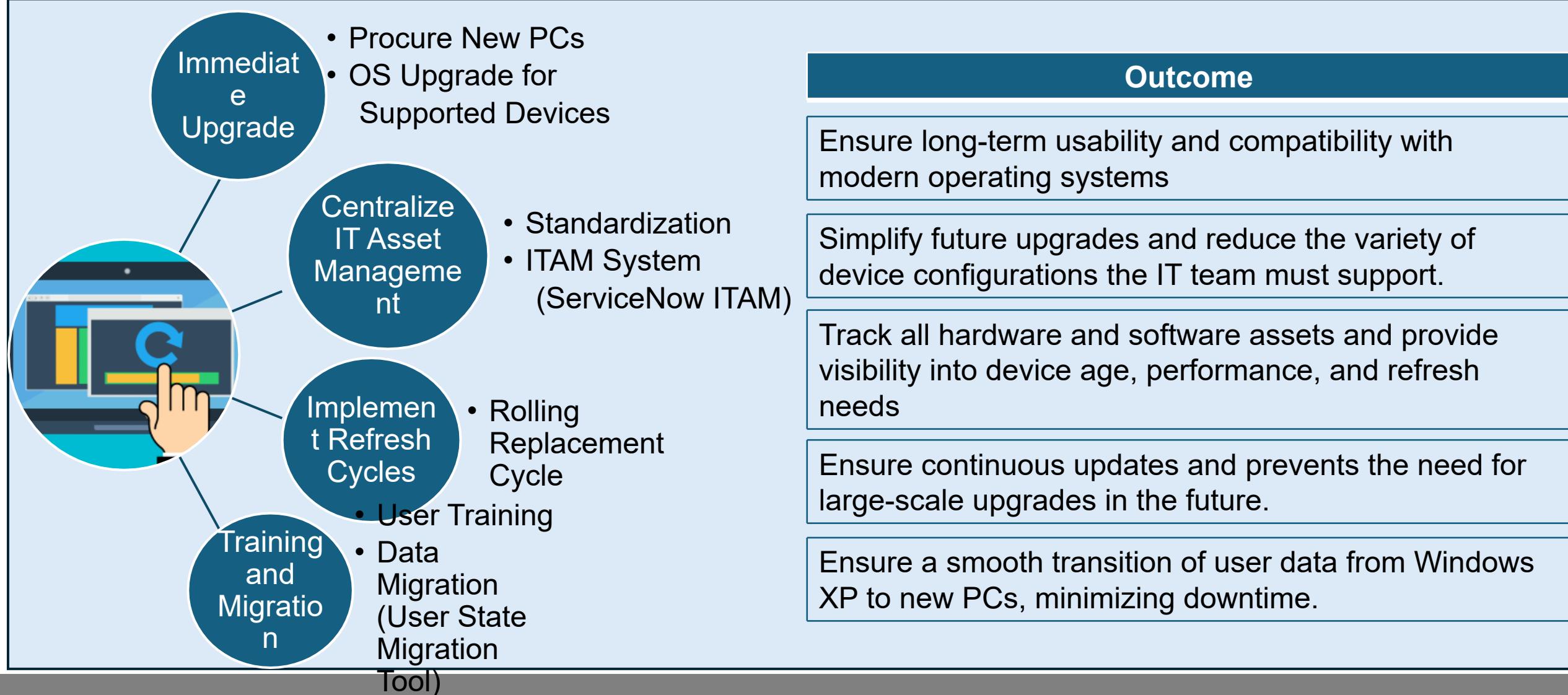
# Current vs. future IT Security structure: lack of leadership vs. centralized CISO



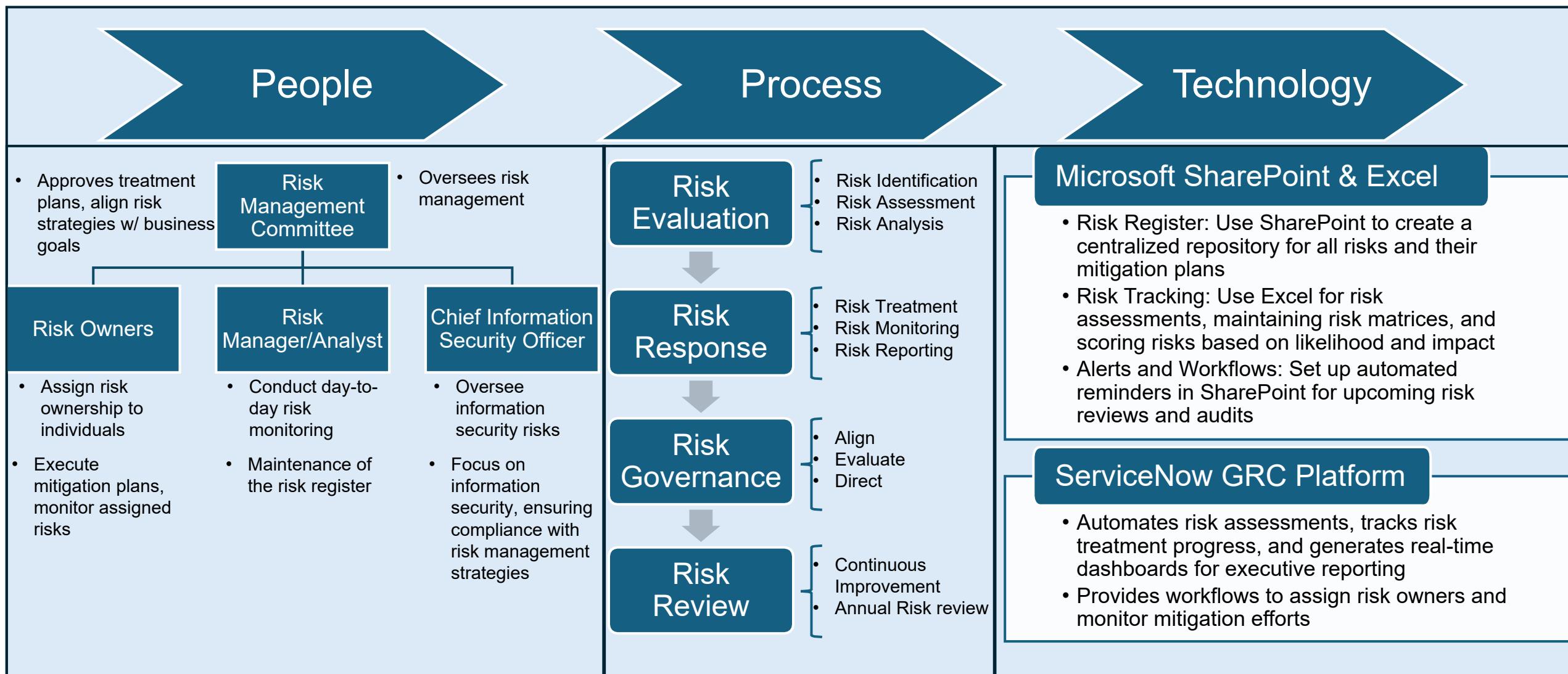
# Seamlessly improving network connectivity with standardized tools



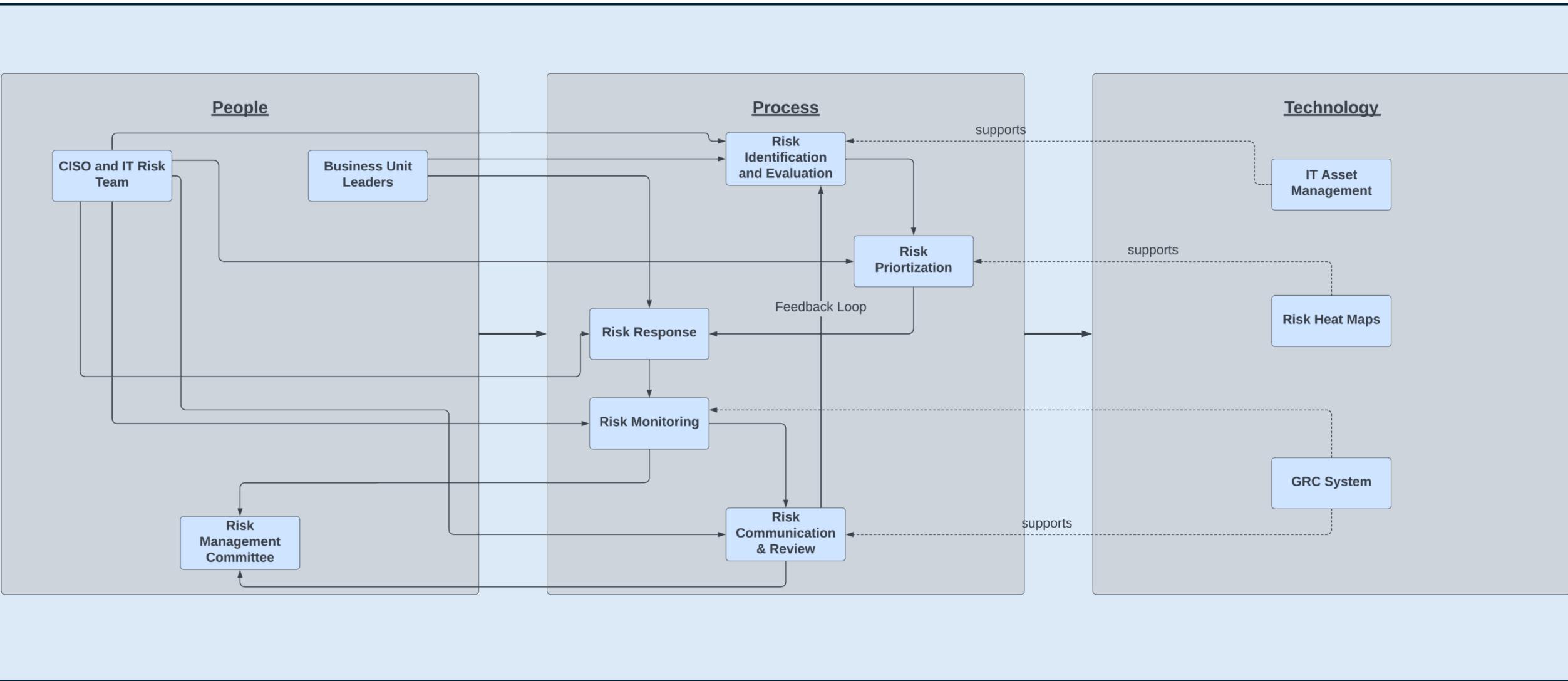
# Replacement of legacy hardware and software



# HG should look at PPT for future risk mitigation strategies

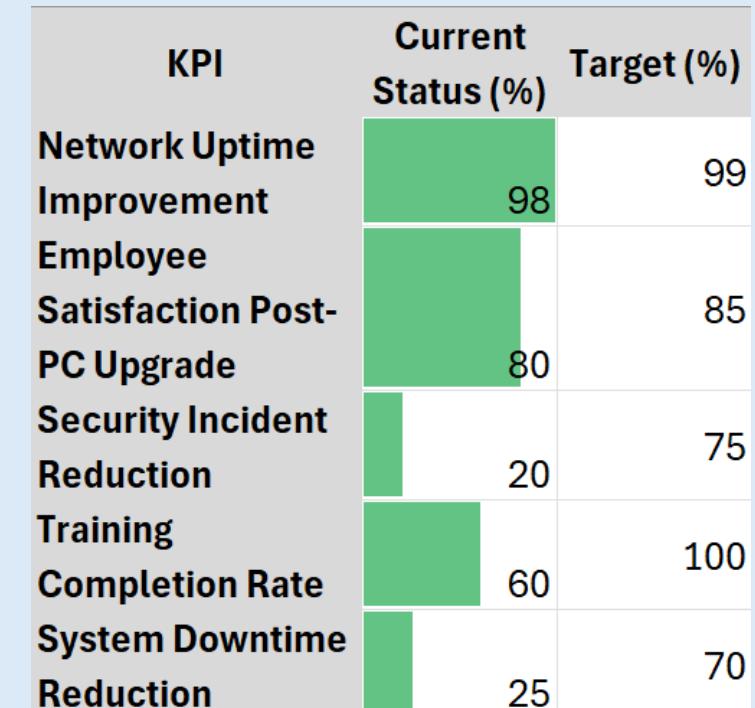


# Visual process flow for continuous risk management



# Implementation and goals for the risk mitigations

Steps:	Year 1											
Hire a CISO												
Hire Full Time Information Security Employees												
Network Assessment												
Upgrade Network Infrastructure												
Immediate PC Upgrade												
Training and Migration												
Standardize Asset Management												



## HG Goals

70% reduction in system downtime within 12 months

## CIO Goals

CISO hired within 6 months

## IT Organization Goals

100% of outdated PCs upgraded in 6 months

# HG will financially breakeven after 2 years of new risk mitigation strategies

## Total Benefits

\$31 million

## Total Costs

\$27 million

### Calculated Metrics:

NPV: \$2,422,278

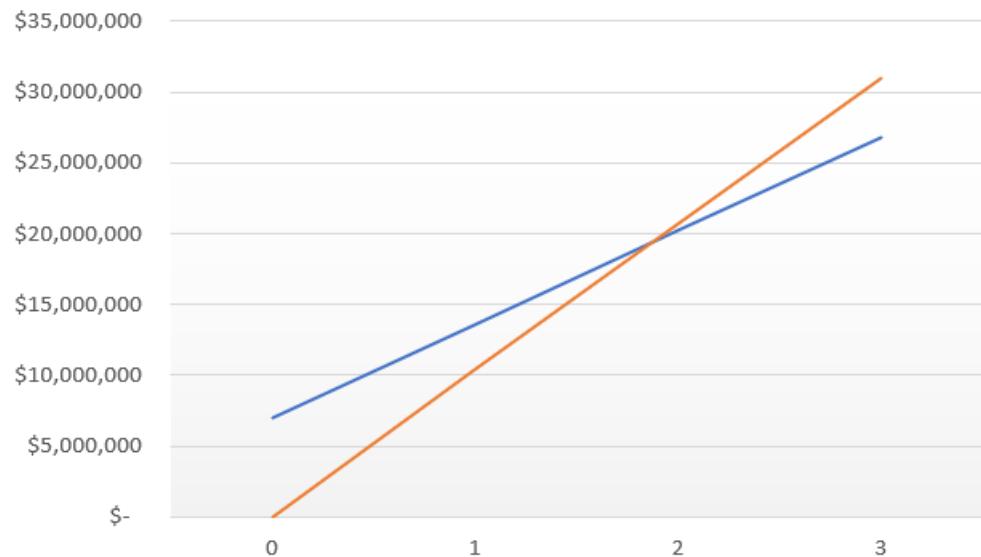
ROI: 16%

### Things to Consider:

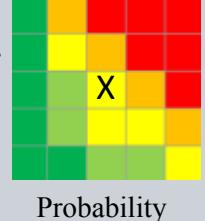
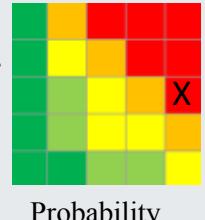
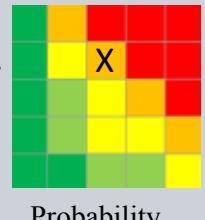
- 3-year scope
- 8,100 employees in total
- 8,300 computers in total
- WACC is 9.45%
- Contractual fines/Downtime avoidance happens every year
- ServiceNow ITAM and GRC included in the estimates for future risk prevention

Cost vs. Benefit

— Cost — Benefit



# Top priority risks and mitigations for HG

Risk	Degree	Mitigation Strategy
<b>Incomplete Risk</b> There is a risk that some critical risks may not be identified during the analysis due to inadequate data collection or overlooked areas in the decentralized environment	Severity  Probability	Implement a comprehensive and structured risk identification process using the ISACA RiskIT framework. Conduct thorough surveys, data collection, and workshops across all business units to ensure all risks are captured
<b>Resistance to Change</b> Business units may resist centralizing IT risk management processes due to concerns over losing control and autonomy	Severity  Probability	Engage key stakeholders early and communicate the benefits of centralization, such as cost savings and improved security. Include them in the design of the process to gain buy-in and ensure smooth implementation
<b>Delayed Risk Treatment</b> Given the scope of HG's IT landscape, delays in implementing risk mitigation strategies may occur, especially in complex areas like ERP consolidation or infrastructure upgrades	Severity  Probability	Prioritize risks based on impact and urgency. Develop a phased approach to implement quick wins first while scheduling more complex mitigations over time. Monitor and track progress closely using risk dashboards

# Stimulating growth for High Gear Engine Company with strategic business decisions supported by IT

**By focusing on these key risks in the process, HG will be well-positioned to manage its IT risks effectively and support its growth trajectory**



## Complete Risk Coverage

- A structured and standardized approach will minimize the likelihood of missing critical risks



## Continuous Risk Monitoring

- Ongoing monitoring will enable HG to stay ahead of emerging risks, ensuring long-term IT resilience



## Timely Mitigation

- A phased implementation strategy will ensure that quick wins are realized while more complex issues are addressed systematically



## Consistency in Risk Assessment

- Standardized criteria will ensure that all business units prioritize risks uniformly



## Stakeholder Buy-In

- Early involvement and transparent communication will ease the transition to a centralized risk management process



## Modern Technology Capabilities

- Replacement of legacy software and hardware enhances security and supports scalability

# Appendices

Financial  
Assumptions

Heat Map

Extended  
Implementation

Network Upgrade

# Risk Score Calculations

Identifier	Description	Risk Score	Risk Impact	Final Score	Reasoning Behind Risk Score	Reasoning Behind Risk Impact
Asset 1	Lack of accountability in security	4.9	5	24.5	The lack of accountability in security poses a severe risk, with a nearly perfect score of 4.9. This issue makes it impossible to enforce proper controls, leaving Atlantic's proprietary processes vulnerable to cyberattacks.	The impact is maximal, with potential consequences including intellectual property theft, regulatory fines, and reputational damage. This poses a significant threat to the company's competitive edge.
Asset 2	Connectivity issues	4.95	5	24.75	The production line at Atlantic Paper Products is heavily dependent on seamless connectivity. Any disruption, even momentary, has a domino effect, leading to production stoppages and delays in fulfilling customer orders. The almost perfect score here reflects how vital this is—every second of downtime equates to massive financial loss, unmet orders, and disgruntled clients.	The risk is not hypothetical—it's a looming threat that could strike at any moment. Given Atlantic's ambition to be the number one paper products producer, even a minor connectivity issue could set the company back significantly in its race to the top.
Asset 3	Fragmented ERP systems	4	3.5	14	Fragmented ERP systems introduce inefficiencies, miscommunication, and delays, becoming a growing drag on performance in a fast-paced and competitive environment.	The impact is less about immediate disaster and more about long-term erosion of operational efficiency, weakening the company's strategic position over time.

# Risk Score Calculations

Identifier	Description	Risk Score	Risk Impact	Final Score	Reasoning Behind Risk Score	Reasoning Behind Risk Impact
Asset 4	Unaddressed audit issues	3.75	4.9	18.375	Atlantic's failure to remediate key audit findings signals deeper control issues. Leaving these issues unresolved puts the company in a precarious position, with potential financial penalties looming.	Unaddressed audit issues are a clear violation of compliance, particularly with Sarbanes-Oxley (SOX) regulations. This could lead to fines, penalties, and undermine investor confidence, posing severe financial and reputational consequences.
Asset 5	Shop floor systems failures	4.5	4.75	21.375	Shop floor systems are crucial for Atlantic's production. Any failure stops production and disrupts operations, leading to delayed shipments, missed commitments, and financial losses.	This could severely impact Atlantic's reputation and long-term profitability.
Asset 6	Legacy software and hardware vulnerabilities	4.85	5	24.25	Atlantic's reliance on outdated systems is a glaring vulnerability. Legacy software and hardware are prime targets for cyberattacks, as they are often unsupported and riddled with security gaps. This isn't just a theoretical risk—it's an invitation for attackers, especially given Atlantic's valuable proprietary processes.	The impact here is catastrophic. A breach caused by legacy vulnerabilities could expose Atlantic to severe data breaches, halting production, and causing regulatory non-compliance. For a company poised to lead the market, a cyber incident could unravel years of progress and tarnish its green technology reputation, leading to legal liabilities, damaged customer trust, and significant financial losses.
Asset 7	Over-reliance on vendors	3.75	3.75	14.0625	This score reflects the delicate balance between benefiting from vendor expertise and exposing the company to risks if those vendors fail to deliver.	Vendor failure can lead to inefficiencies, delays, and potential quality issues, damaging customer relationships and delaying critical projects. Over time, this weakens the company's agility and responsiveness to market demands.

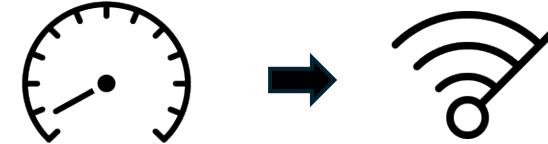
# Extended implementation including proposed risk analysis

Phases:	Year 1											
Risk Analysis												
Hire a CISO												
Hire Full Time Information Security Employees												
Network Assessment												
Upgrade Network Infrastructure												
Immediate PC Upgrade												
Training and Migration												
Standardize Asset Management												
Future Risk Analysis												

# Network Connectivity and Infrastructure Issues

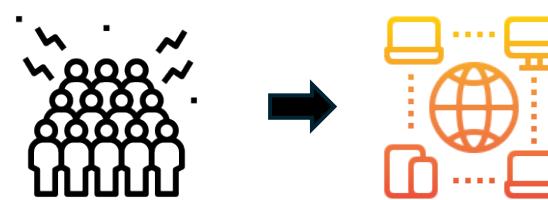
## Network Assessment and Optimization

- Network Audit: Identify bandwidth usage patterns, bottlenecks, and peak traffic times
- Bandwidth Segmentation: Implement QoS to prioritize traffic for critical applications



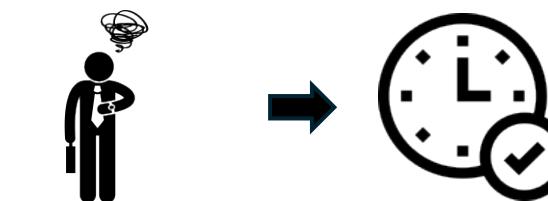
## Upgrade Internet Bandwidth and Network Infrastructure

- Bandwidth Increases: Implement dedicated internet line and update ISP SLAs for higher bandwidth availability
- Network Equipment Upgrade: Implement enterprise-grade switches that support Gb Ethernet, or redundant internet connections from multiple ISPs



## Cloud Readiness and Network Optimization

- Cloud Readiness Assessment: Identify which systems can be optimized for cloud environments and implement WAN for better latency and performance
- Wi-Fi Optimization: Upgrade Wi-Fi systems to support Wi-Fi 6 or 7



# Estimated cost savings for enhancing connectivity

Assumption	Value	TOTAL SAVINGS
Affected Employees	500	\$ 2,437,500.00
Time Wasted per Day (Hours)	0.5	
Hourly Wage (USD)	50	
Workdays per Year	260	
Productivity Recovered (%)	0.75	

# Financial Analysis

Period (e.g. Year)	0	1	2	3	4	5	
Net Cash Flows (NCF)	\$ (7,007,079)	\$ 3,755,239	\$ 3,755,239	\$ 3,755,239	\$ -	\$ -	
NPV (Annual)	\$ (7,007,079)	\$ 3,430,908	\$ 3,134,588	\$ 2,863,861	\$ -	\$ -	
ROI (Running Total)		-100%	-24%	2%	16%	16%	16%
							Break Even
<b>Costs</b>							
<b>One-Time (Non-recurring)</b>							
Salaries consults for Network Audit	\$ 453,600	R_f		4.06% LT debt	2100000000		
Initial purchase price of OS	\$ 1,153,700	ERP		4.60% Market cap	4150000000		
Initial purchase price of Computers	\$ 4,565,000	beta		1.57 E.Tax Rate	18.90%		
Salaries consultants for Network Audit	\$ 453,600	R_S		11.28200%			
Initial purchse price of network gear	\$ 63,979	Credit Spread for B+ Credit Rating		0.0314			
Wi-Fi router Upgrade	\$ 166,000	R_B		7.20%			
Cloud Readiness assessment Consulting fee & salary	\$ 151,200						
<b>One-Time Costs per Period</b>	<b>\$ 7,007,079</b>						<b>\$ 7,007,079</b>
<b>Recurring</b>							
	Often begin after "go-live", e.g. Period 1 or 2						
CISO Salary	\$ -	\$ 334,111	\$ 334,111	\$ 334,111			
Security Analyst Salary	\$ -	\$ 990,000	\$ 990,000	\$ 990,000			
ISP Bandwidth Increase cost	\$ -	\$ 3,600,000	\$ 3,600,000	\$ 3,600,000			
ServiceNow ITAM and QoS	\$ -	\$ 1,660,000	\$ 1,660,000	\$ 1,660,000			
<b>Recurring Costs per Period</b>	<b>\$ -</b>	<b>\$ 6,584,111</b>	<b>\$ 6,584,111</b>	<b>\$ 6,584,111</b>			<b>\$ 19,752,333</b>

Introduction

Recommendations

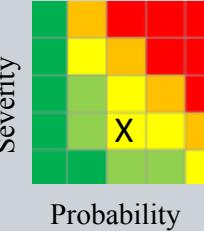
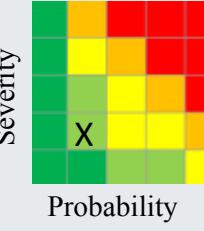
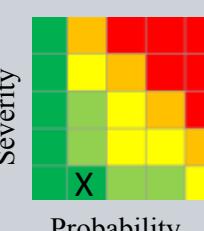
Implementation

Financials

Risks & Mitigation

Conclusion

# Other risks to consider and mitigation strategy for HG

Risk	Degree	Mitigation Strategy
<b>Inconsistent Risk Assessment</b> Different business units may have varying interpretations of risk severity, leading to inconsistent prioritization	Severity  Probability	Standardize the risk assessment methodology across all units, utilizing clear criteria for impact and likelihood. Train the risk management team on consistent scoring to ensure uniform risk evaluation
<b>Lack of Continuous Monitoring:</b> Once risks are mitigated, there is a risk that the organization will fail to continuously monitor new and evolving risks	Severity  Probability	Implement an ongoing risk monitoring program with regular reviews and updates. Use automated tools for real-time monitoring and reporting, ensuring risks are continuously managed.
<b>Inadequate Resource Allocation:</b> The risk management process may be hindered if insufficient resources (personnel, tools, or budget) are allocated to identify, assess, and mitigate risks across HG's decentralized business units	Severity  Probability	Ensure proper resource allocation by aligning the risk management budget with business priorities. Assign dedicated personnel to key areas of the risk management process, and consider using interim solutions such as Microsoft SharePoint or Excel for risk tracking until more robust tools can be implemented

# Financial Analysis

## Benefits

### Cost reduction

### Cost avoidance

Ransomware Avoidance

Data Breach Avoidance

No contractual fines due to downtime

No payment to Third-party OS support

	\$		\$	1,335,000	\$ 1,335,000	\$ 1,335,000
			\$	554,250	\$ 554,250	\$ 554,250
			\$	5,000,000	\$ 5,000,000	\$ 5,000,000
	\$	- \$	\$	1,012,600	\$ 1,012,600	\$ 1,012,600

### Value/revenue enhancement

Increased Productivity

	\$		\$	2,437,500	\$ 2,437,500	\$ 2,437,500
--	----	--	----	-----------	--------------	--------------

### Total Benefits per Period

### Cumulative Benefits

\$	- \$	10,339,350	\$10,339,350	\$10,339,350	\$31,018,050
\$	- \$	10,339,350	\$20,678,700	\$31,018,050	\$62,036,100

ROI	16%
NPV	\$2,422,278
IRR	28%

NPV	\$2,422,278
-----	-------------