

Cybersecurity Risk Management Program – BSI



PREPARED FOR THE
BOARD OF DIRECTORS



PRESENTED BY:
AUSTIN J

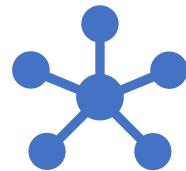


JANUARY 2026

Business Context



- Regional retail organization



- Centralized IT infrastructure



- Financial, HR, and customer data

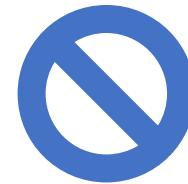
Why Risk Management Is Needed



- Increased cyber threats



- Business disruption risk



- No formal risk program

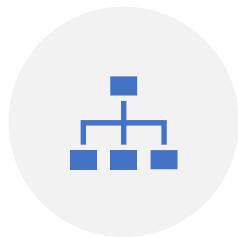
Current Risk Challenges

- No defined risk ownership

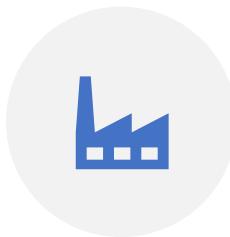
- Limited risk assessments

- Controls not aligned to risk

Recommended Framework



NIST RISK
MANAGEMENT
FRAMEWORK (RMF)



- INDUSTRY STANDARD



- SCALABLE



- BUSINESS-ALIGNED

RMF Lifecycle

- Categorize systems

- Select controls

- Implement controls

- Authorize risk

- Monitor continuously

Applying RMF at BSI

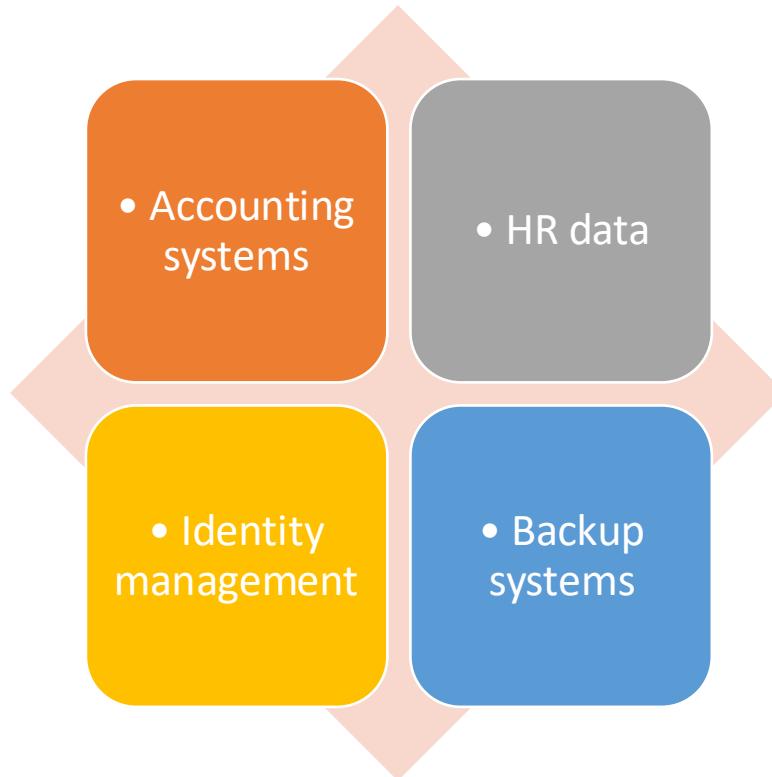
- Identify assets

- Assess threats

- Evaluate impact

- Make risk decisions

Key Information Assets



Asset Prioritization



- CONFIDENTIALITY



- INTEGRITY



- AVAILABILITY



- WEIGHTED RANKING

Key Threats



- RANSOMWARE



- DATA BREACH

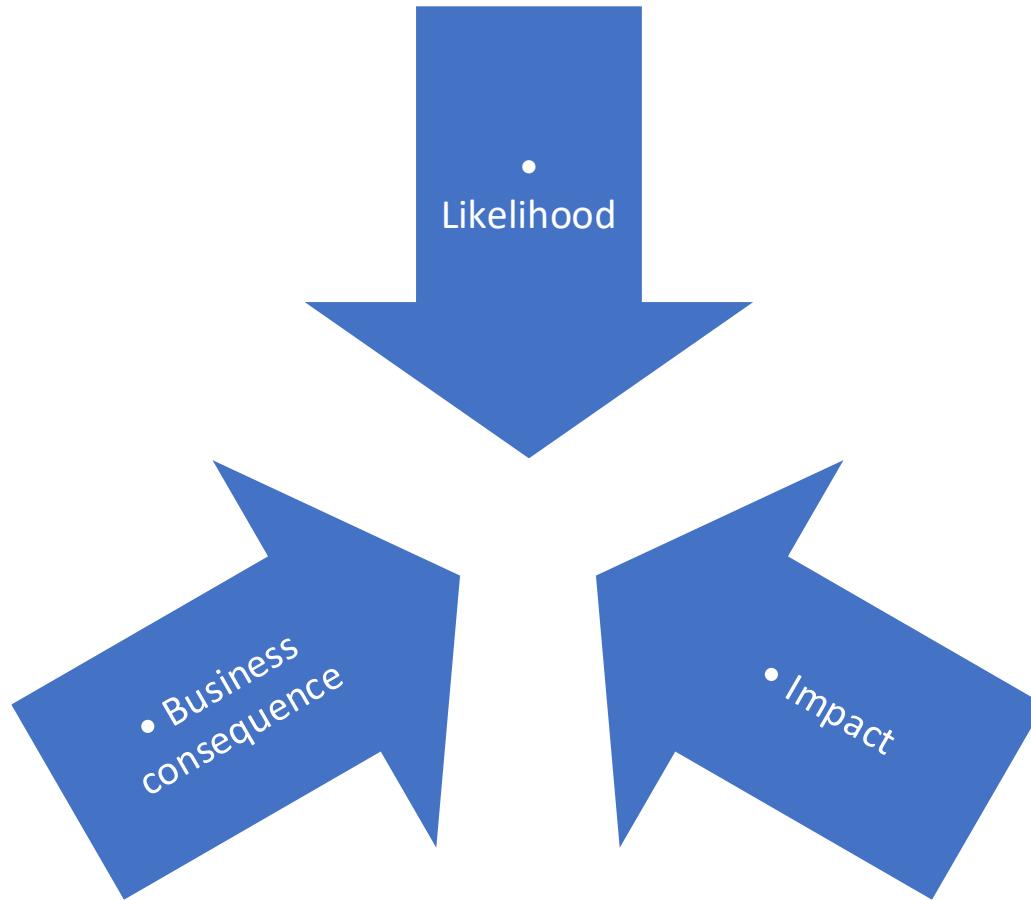


- UNAUTHORIZED
ACCESS



- INSIDER MISUSE

Threat Prioritization



Risk Analysis

- Likelihood × Impact
- Identifies highest risks



Governance Model

- Board oversight

- Executive ownership

- IT execution

Program Benefits



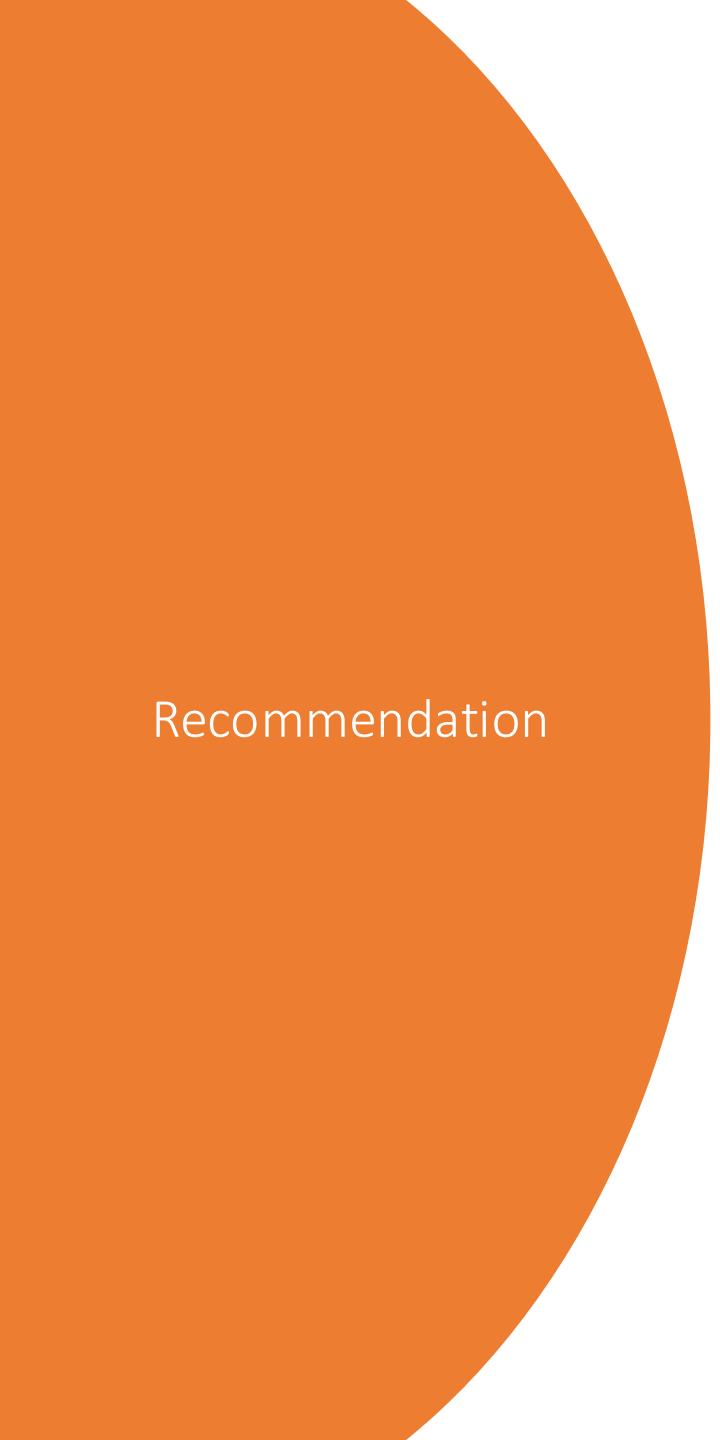
- Reduced risk



- Accountability



- Improved resilience

A large orange circle is positioned on the left side of the slide, overlapping the white background. It is centered vertically and has a slight shadow, giving it a 3D appearance.

Recommendation

- Adopt NIST RMF
- Formalize governance
- Begin continuous risk management