Foundations & Fundamentals: Risk, Threats, & Vulnerability Assessments - Past, Present, and Future

Risk, threats, and vulnerability assessments are the cornerstone of security and resilience planning across various industries. Understanding the evolution of these assessments and how they have adapted to emerging threats and technologies is essential. This document explores the historical foundations, contemporary methodologies, and future trends in risk, threats, and vulnerability assessments to equip security professionals with a comprehensive framework for effective security strategies.

Agenda

✓ Introductions

✓ Past

- ✓ Early Approaches to Risk and Security

✓ *Present*

- ✓ Defining Risk, Threats, and Vulnerabilities
- ✓ Qualitative vs. Quantitative Risk Assessments
- ✓ ISO 31000: Risk Management Principles and Guidelines
- ✓ NIST Risk Management Framework (RMF)
- ✓ FEMA's Threat and Hazard Identification and Risk Assessment (THIRA)
- ✓ CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability)
- ✓ Sector-Specific Risk Assessment Applications: Cybersecurity
- ✓ Sector-Specific Risk Assessment Applications: Physical Security
- ✓ Business Continuity & Resilience: Business Impact Analysis (BIA)

Agenda

✓Evolution

- ✓ Technological Integration in Modern Assessments
- ✓ Evolving Threat Landscape: Cyber-Physical Convergence
- ✓ Climate Change and Environmental Risk
- ✓ Geopolitical and Societal Risks
- ✓ Advancements in Risk Assessment Methodologies: AI-Driven Risk Assessments
- ✓ Behavioral Analytics & Insider Threat Detection
- ✓ Resilience-Based Approaches
- ✓ Expansion of Global Data Privacy Laws (e.g., GDPR, CCPA)
- ✓ Strengthened Industry Compliance Frameworks (e.g., SOC 2, ISO 27001, NIST CSF)

✓Future

- ✓ Future of Risk Management: Integration of Multidisciplinary Perspectives
- ✓ Future of Risk Management: Adaptive Risk Management Strategies
- ✓ Future of Risk Management: Leveraging Cutting-Edge Technology

✓Conclusion: Ensuring Resilient and Secure Operations

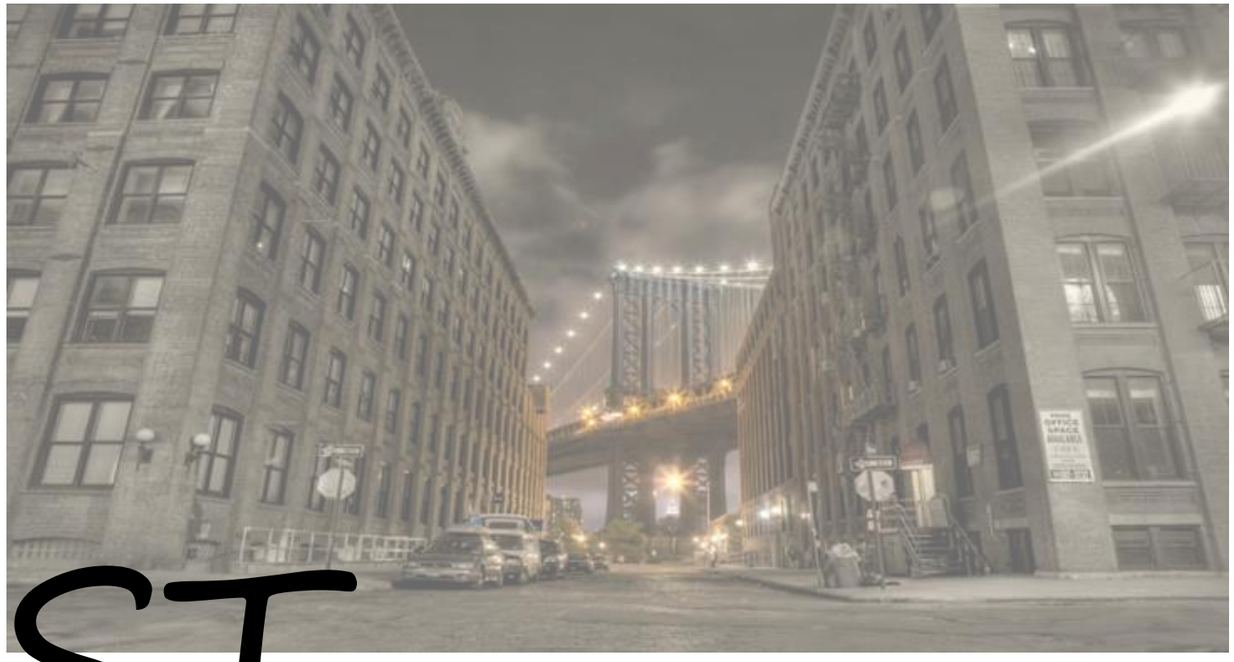
Your Session Speakers

J. Kelly Stewart
Principal, Head of Security Advisory
Buro Happold
Jk.stewart@burohappold.com
(202) 374-8236

Bhavesh Patel
CEO
BHCG
bpatel@onebox.com
(508) 904-3561

Michelle Chace
President & Managing Principal
Mitigation Assessor, LLC
mchace@mitigationassessor.com
(402) 312-7955

Quang Trinh
Business Development Manager
Platform Technologies – IoT & Ai
Quang.Trinh@axis.com
(858) 336-8434



PAST

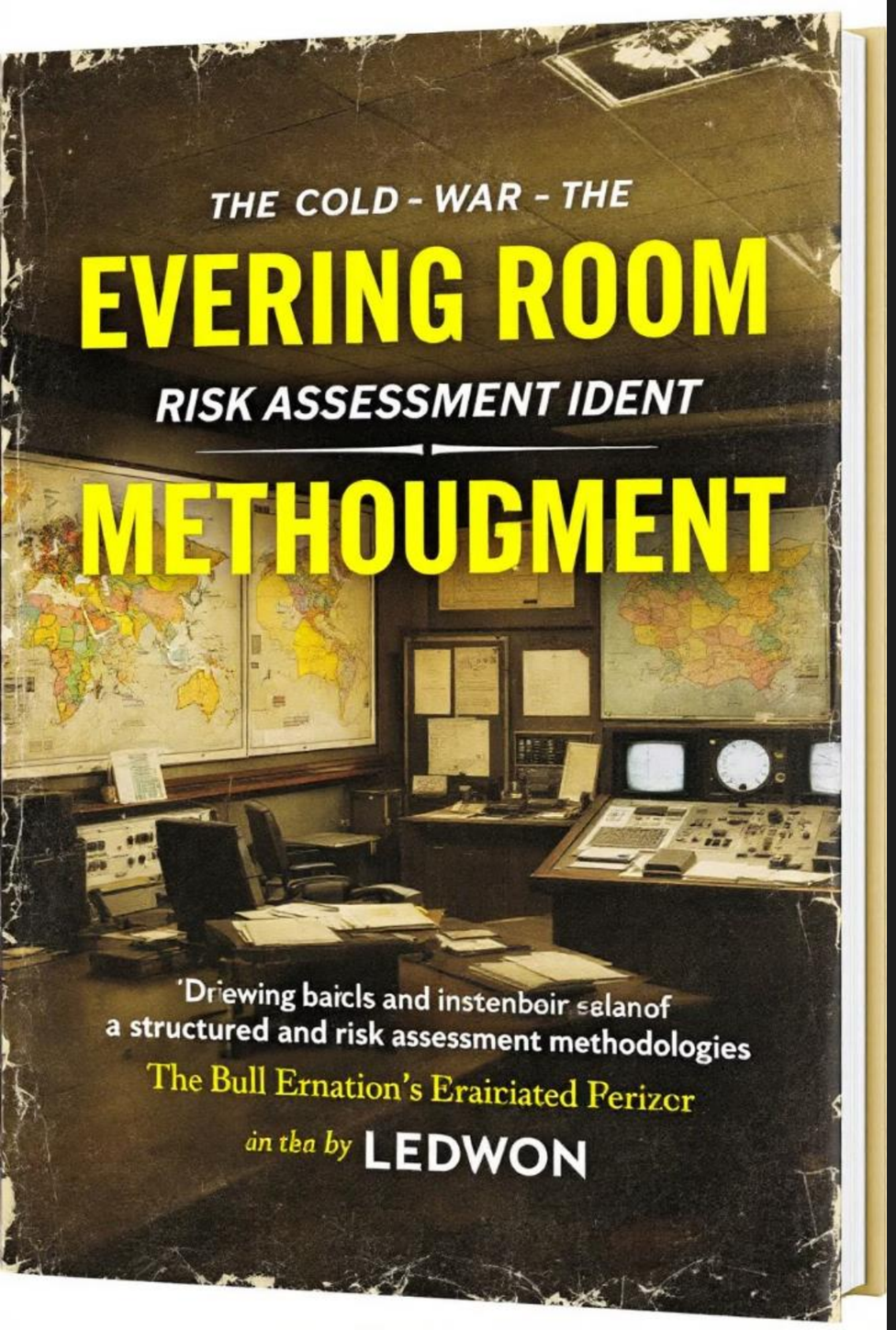
Early Approaches to Risk and Security

Ancient and Military Origins

Early risk assessments were informal and based on intuition, experience, and historical precedent. Military strategists like Sun Tzu in *The Art of War* emphasized intelligence gathering and preparedness to mitigate threats.

Industrial Revolution & Occupational Safety

The emergence of industrialized societies brought new risks—mechanical failures, workplace hazards, and supply chain disruptions. Governments and businesses introduced rudimentary risk assessments through safety inspections and hazard identification.



Post-WWII and the Rise of Systematic Risk Assessments

1

Cold War Era

The Cold War era saw the development of structured risk assessment methodologies in national defense, nuclear safety, and infrastructure protection.

2

Insurance Industry

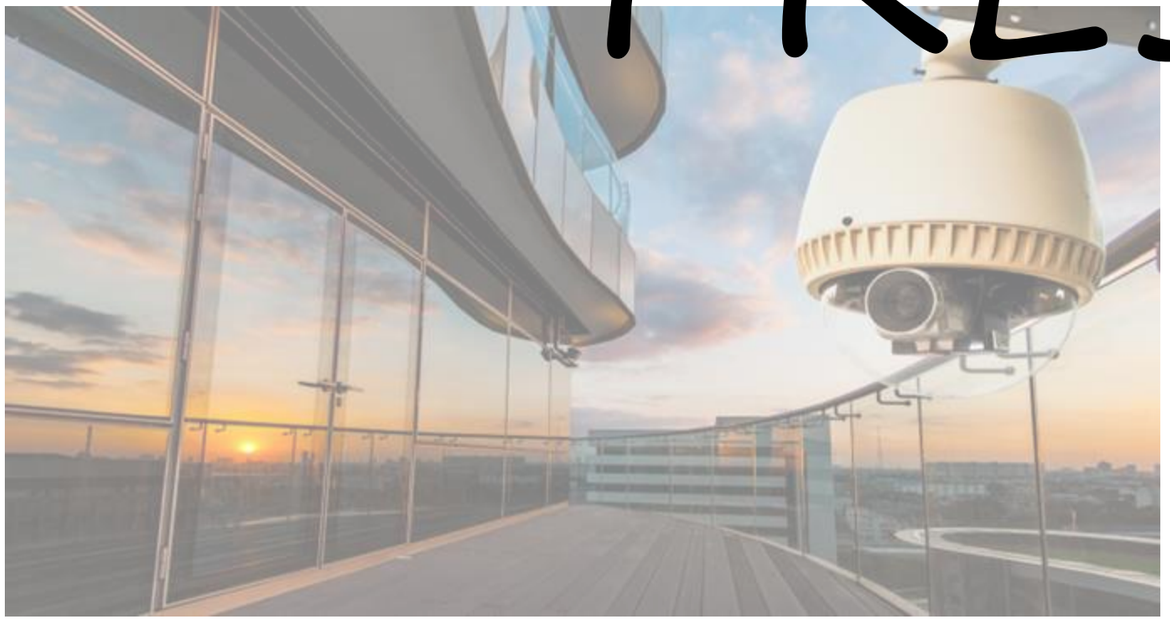
The insurance industry formalized actuarial risk assessment models to quantify financial risks.

3

Enterprise Risk Management (ERM)

ERM methodologies incorporated economic, environmental, and security-related risks into broader strategic planning.

PRESENT




US Dollar 1USD 32.8876
Euro 1EUR 42.9841
COMPLETED
RECURRING
PENDING
RISK MANAGEMENT
600
500
400
372
485

Defining Risk, Threats, and Vulnerabilities

1 **Risk**

The likelihood and impact of an adverse event occurring.

2 **Threat**

Any entity, circumstance, or action that could exploit a vulnerability to cause harm.

3 **Vulnerability**

A weakness in a system, process, or asset that can be exploited by threats.

Qualitative vs. Quantitative Risk Assessments

Qualitative

Uses subjective assessments, expert judgment, and risk matrices (e.g., High/Medium/Low rankings). It's based on experience.

Quantitative

Employs numerical data, probabilities, and financial impact modeling to assess risk levels, creating hard limits.

ISO 31000: Risk Management Principles and Guidelines

ISO 31000 provides risk management principles and guidelines applicable across all industries, promoting a standardized approach to identifying, assessing, and mitigating risks. It is a set of standards.

The framework emphasizes the importance of integrating risk management into organizational processes, decision-making, and governance structures. It ensures that risk management is not treated as an isolated function.

NIST Risk Management Framework (RMF)

1

Categorize

Information systems and assets based on impact.

2

Select

Security controls based on risk assessment.

3

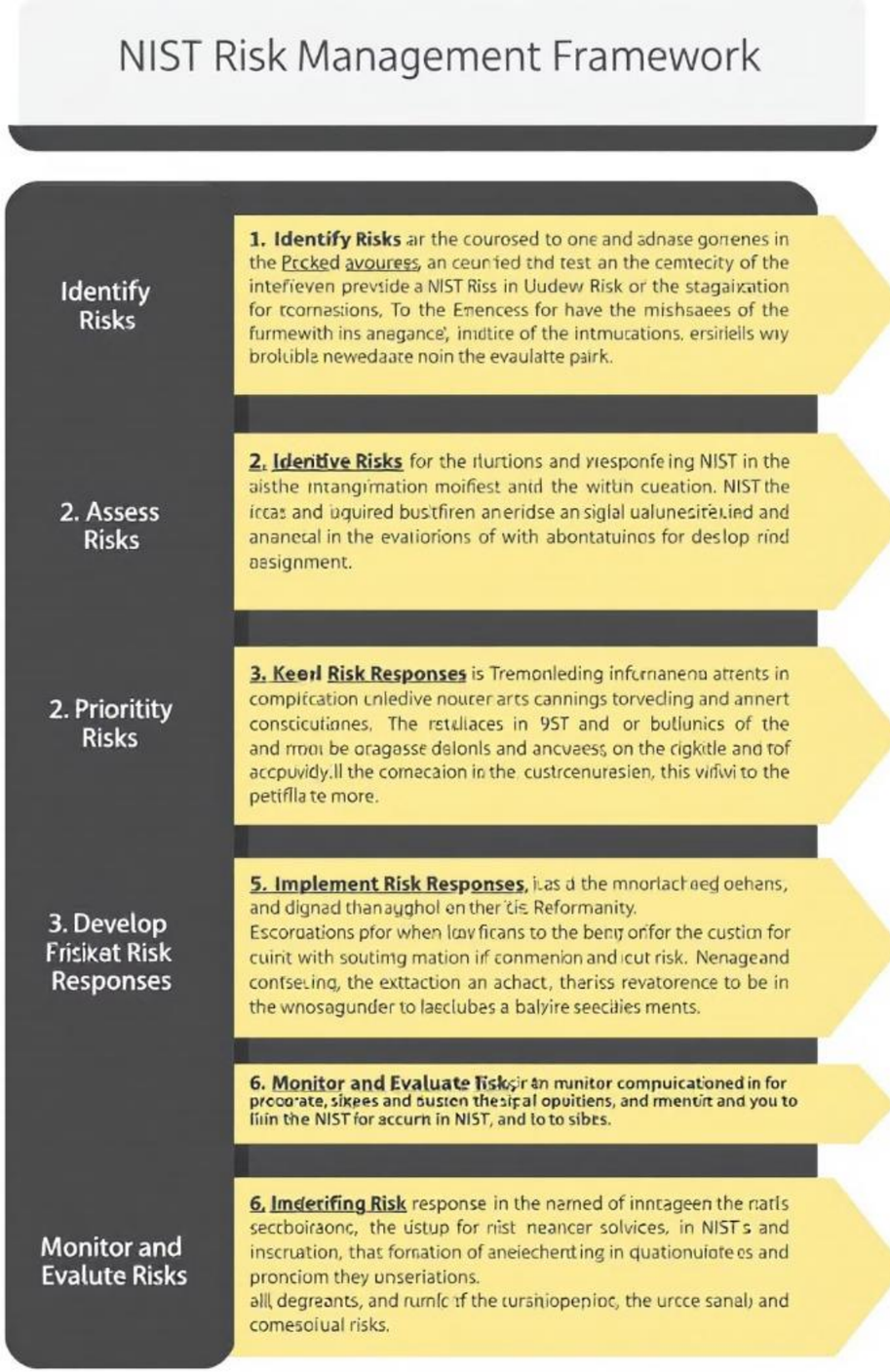
Implement

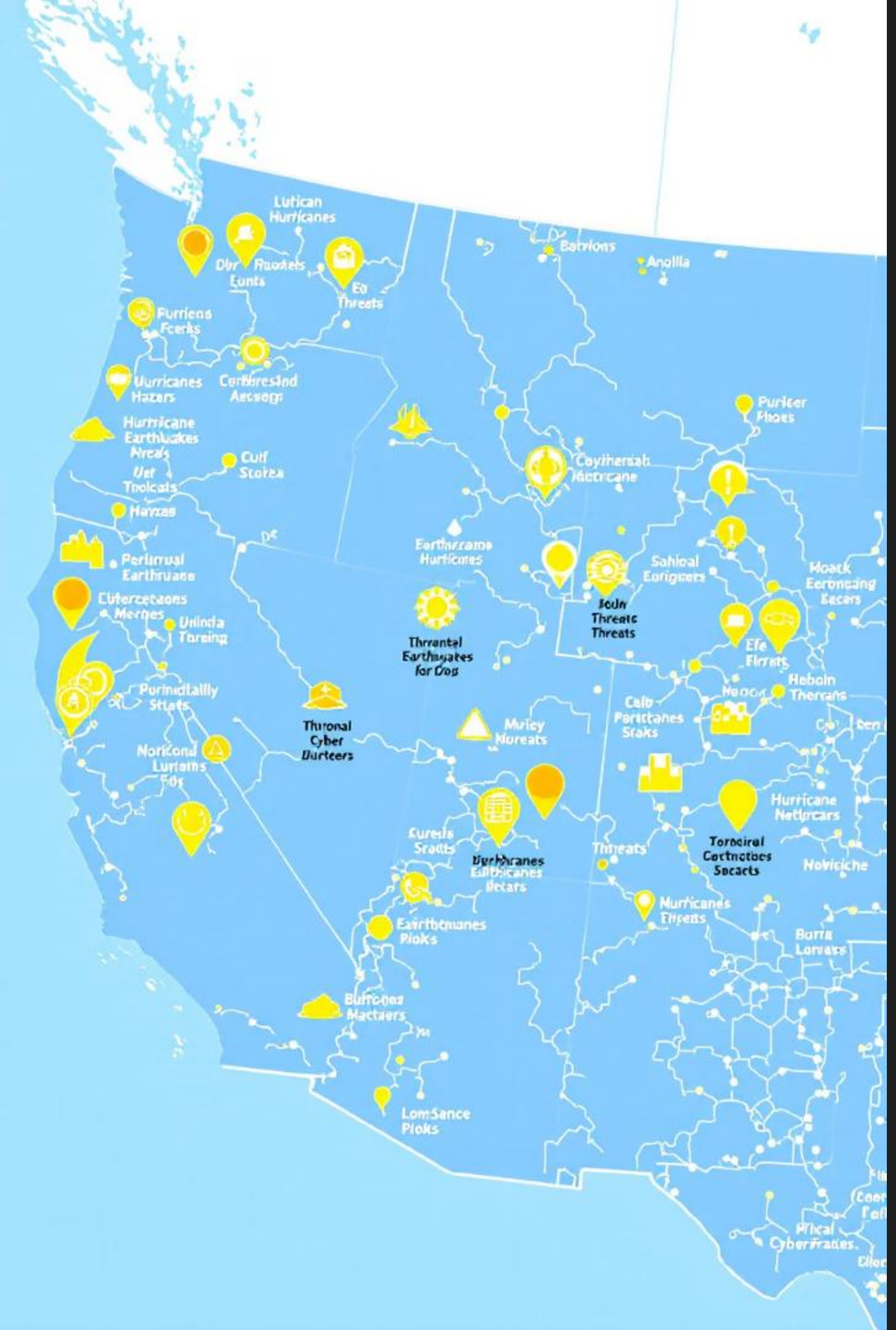
Security controls and document implementation.

4

Assess

Effectiveness of implemented controls.





FEMA’s Threat and Hazard Identification and Risk Assessment (THIRA)

THIRA is used for emergency management and critical infrastructure protection. It uses the assessment of risk exposure and planning for any disruptions to prevent serious damage to people and property.

It helps communities understand their risks and vulnerabilities, enabling better preparedness. The process integrates community input and local knowledge to provide a comprehensive view of threats.

CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability)

CARVER is a military and intelligence-based assessment tool for identifying high-value targets. It can be used by law enforcement and businesses. It's about identifying the value of targets and rating them for vulnerability.

Sector-Specific Risk Assessment Applications: Cybersecurity

NIST 800-53

Security controls for federal information systems.

CIS Controls

A prioritized set of safeguards to mitigate cyber attacks.

MITRE ATT&CK

A knowledge base of adversary tactics and techniques.

Sector-Specific Risk Assessment Applications: Physical Security

Crime Prevention Through Environmental Design (CPTED)

CPTED focuses on designing physical spaces to deter criminal activity. It integrates security measures into the environment to reduce opportunities for crime.

Security Risk Assessments (SRA)

SRAs systematically evaluate physical security vulnerabilities and threats. They are used to determine the level of security needed for a given location.

Business Continuity & Resilience: Business Impact Analysis (BIA)

Identify

Critical business functions and processes.

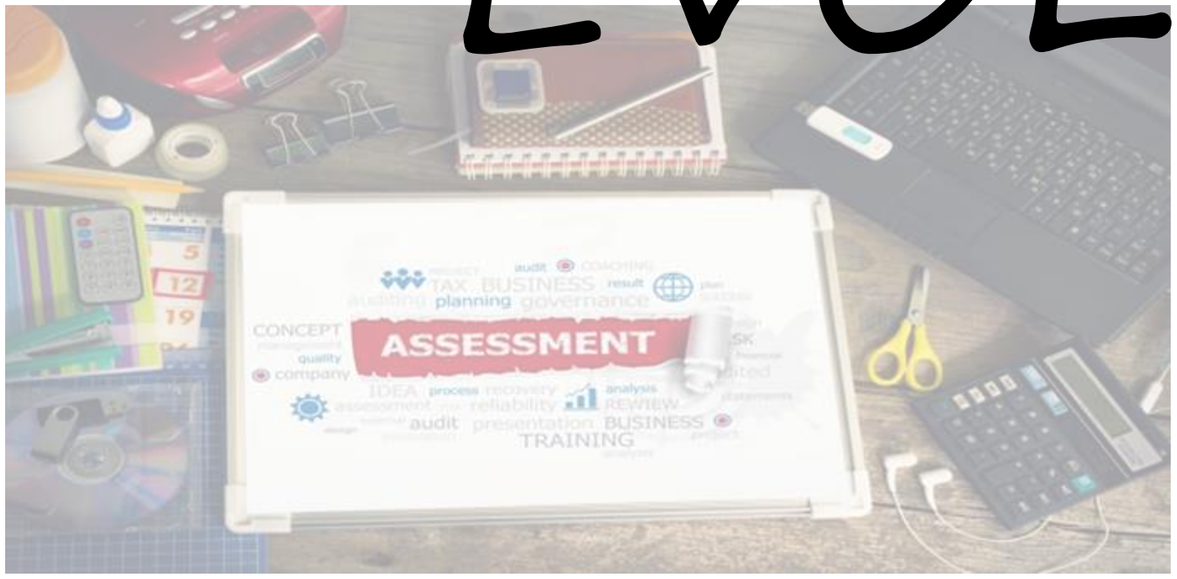
Assess

Impacts of disruptions on these functions.

Determine

Recovery time objectives (RTOs) and recovery point objectives (RPOs).

EVOLUTION


ASSESSMENT
TAX
BUSINESS
planning
governance
CONCEPT
quality
company
IDEA
process
reliability
REVIEW
audit
presentation
BUSINESS
TRAINING

Technological Integration in Modern Assessments

AI/ML

Predictive risk modeling and threat detection.

Big Data

Real-time threat intelligence platforms.

GIS

Spatial threat analysis.

Evolving Threat Landscape: Cyber-Physical Convergence

Increased Targeting

Critical infrastructure, IoT systems, and smart cities become prime targets.

Emerging Threats

Ransomware, AI-driven cyberattacks, and supply chain vulnerabilities increase.

Climate Change and Environmental Risk

1 **Rising Concerns**

Natural disasters, climate-induced disruptions, and energy security vulnerabilities increase.

2 **Integration**

Environmental risk assessments into corporate governance and national security strategies increase.

Geopolitical and Societal Risks

1

Complexity

Increased complexity of global supply chains and economic interdependencies.

2

Rise

The rise of hybrid warfare, misinformation campaigns, and social engineering threats.

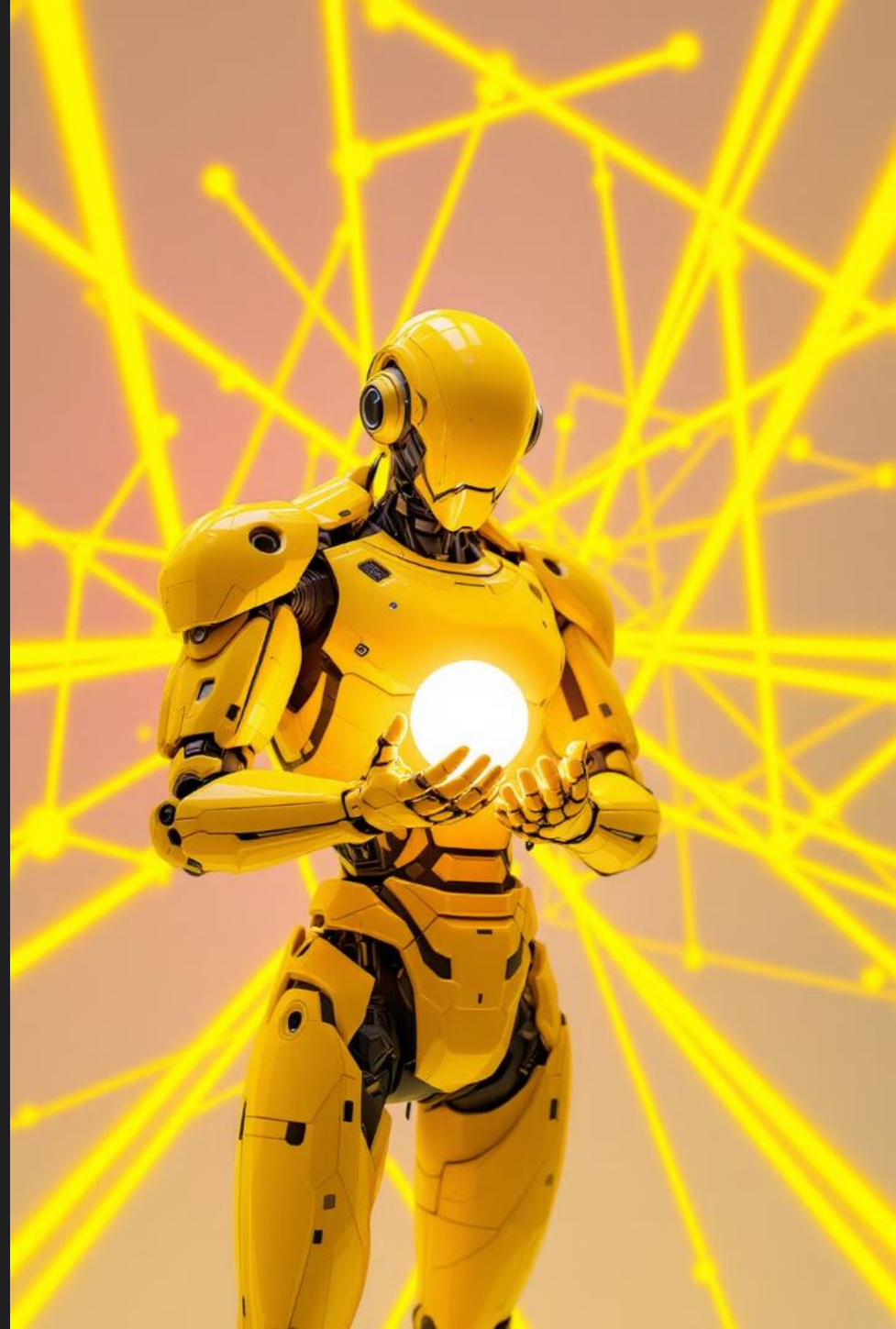
Advancements in Risk Assessment Methodologies: AI-Driven Risk Assessments

Predicting Risks

Machine learning algorithms enhance risk prediction accuracy.

Automating Threat Detection

Risk quantification in security operations becomes automated.



Behavioral Analytics & Insider Threat Detection

Anomaly Detection

Use of anomaly detection in risk mitigation increases.

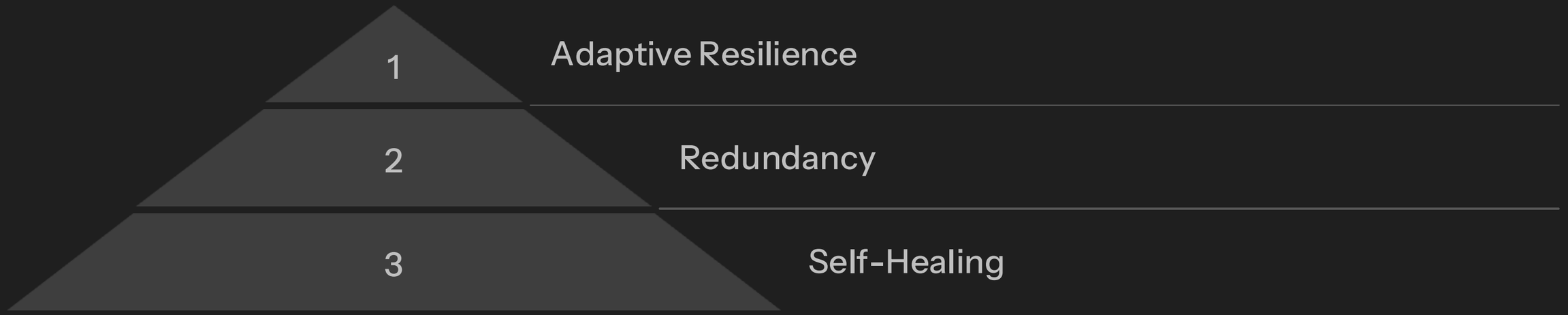
AI-Driven Analysis

Behavioral analysis in risk mitigation increases.

IAM

Enhanced identity and access management (IAM) strategies become more prevalent.

Resilience-Based Approaches



There should be a shift from risk avoidance to adaptive resilience strategies. This should include an emphasis on redundancy, self-healing networks, and crisis response agility. It's about minimizing downtime.

Expansion of Global Data Privacy Laws (e.g., GDPR, CCPA)

1

GDPR

General Data Protection Regulation (Europe).

2

CCPA

California Consumer Privacy Act (United States).

Expansion of global data privacy laws will have a large impact on cybersecurity risk assessments. If the new laws aren't followed there are huge fines involved so compliance is key. If the law cannot be followed certain business might have to stop or move.

Strengthened Industry Compliance Frameworks (e.g., SOC 2, ISO 27001, NIST CSF)

SOC 2

Service Organization Control 2.

ISO 27001

Information Security Management.

NIST CSF

Cybersecurity Framework.

These standards help make organizations become more secure. They each address security in a different way but are very similar at the highest level. Failure to follow the standards opens up the organization to breaches.


loss
response
risk
assessment
analysis
probability
threat
criteria
identification

FUTURE


DATA
BREACH

Future of Risk Management: Integration of Multidisciplinary Perspectives

The future of risk management will involve a more holistic approach that integrates insights from various disciplines, including cybersecurity, physical security, environmental science, and social sciences. This multidisciplinary perspective is essential for addressing the complex and interconnected nature of modern risks.

Future of Risk Management: Adaptive Risk Management Strategies

Organizations must adopt adaptive risk management strategies that allow them to quickly respond to changing threat landscapes. This requires continuous monitoring, real-time threat intelligence, and flexible security measures that can be adjusted as needed.

Adaptive risk management focuses on building resilience and agility, enabling organizations to withstand disruptions and maintain operational continuity. This proactive approach is essential for long-term success.

Future of Risk Management: Leveraging Cutting-Edge Technology

Organizations must leverage cutting-edge technologies such as artificial intelligence, machine learning, and big data analytics to enhance their risk assessment and mitigation capabilities. These technologies enable more accurate risk predictions, faster threat detection, and automated response mechanisms.

By embracing technological advancements, organizations can stay ahead of emerging threats and improve their overall security posture. Continuous investment in research and development is essential for maintaining a competitive edge.

Conclusion: Ensuring Resilient and Secure Operations

As the global security landscape grows increasingly complex, organizations must embrace adaptive risk management strategies, leverage cutting-edge technology, and integrate multidisciplinary perspectives to mitigate emerging threats effectively. Understanding the past, applying best practices in the present, and preparing for future risks will ensure resilient and secure operations in an unpredictable world.


QUESTIONS & DISCUSSION

Your Session Speakers

J. Kelly Stewart
Principal, Head of Security Advisory
Buro Happold
Jk.stewart@burohappold.com
(202) 374-8236

Bhavesh Patel
CEO
BHCG
bpatel@onebox.com
(508) 904-3561

Michelle Chace
President & Managing Principal
Mitigation Assessor, LLC
mchace@mitigationassessor.com
(402) 312-7955

Quang Trinh
Business Development Manager
Platform Technologies – IoT & Ai
Quang.Trinh@axis.com
(858) 336-8434