CYIENT

# REIMAGINING RISK: AUTOMATING CYBERSECURITY RISK ASSESSMENTS WITH GENAI

A practical approach to simplifying cybersecurity risk assessments with GenAI—reducing time, effort, and complexity.

# Contents

## Abstract

Risk assessment automation using GenAI streamlines the identification, evaluation and management, of cybersecurity risks. Tasks such as data collection, identifying the known threats and vulnerabilities detection, risk analysis, risk prioritization, remediation suggestions and reporting are automated to enhance efficiency, consistency, and accuracy. The framework reduces human error and enables a more proactive approach to cyber risk management. As risk profiles evolve, the automation engine must be periodically updated to maintain accuracy.

The GenAI -based solution allows risk assessments to be conducted quickly and effectively. It reduces manual effort and generate reports in preferred formats. Most assets include components with known vulnerabilities, which can be fetched from the NVD (National Vulnerability Database). Threats and associated risks are identified through scripting and GenAI. Since risk assessments must be repeated periodically to meet regulatory needs or address platform changes, automation significantly reduces time and effort. This paper details the automation for risk assessment as against the conventional manual methodology.


## Introduction

Risk assessment automation is enabled by an engine that include known threats, commonly known vulnerabilities, and associated risks for commonly used information assets. Approximately 70% of assets and their associated risks, vulnerabilities, and threats remain consistent across assessments, allowing automation to eliminate redundancy and improve accuracy.

Risk assessment is critical across domains such as automotive, healthcare, energy, mining, utilities. Identifying the security risks early and taking remediation actions helps reduce cyber threats. With Dynamic risks driven by evolving technologies and regulations, Gen AI enables rapid risk scoring and report generation. Reports are then reviewed to eliminate the false positives and tailor insights to the specific environment.

## Problem Definition

Traditional risk assessments require significant manual effort and time. Automation not only reduces this burden, but also delivers precise and actionable insights.

## Why Risk Assessments Must Evolve

Risk assessment help identify security risks associated with assets across domains. They are essential for compliance with industry standards such as ISO 27001, ISO 31000, ISO 14971, and must be conducted annually or at predefined intervals.

For the automotive sector, Threat Analysis and Risk Assessment (TARA) is required to comply with ISO 21434. These assessments help determine residual risks, define security goals and derive cybersecurity requirements. In healthcare, assessments must align with ISO 14971 to meet FDA mandates. OT security assessments are guided by IEC 62443.

Cyient's accelerator solution- **CySecAssure** - streamlines risk assessments by reducing manual effort and quickly generating draft reports. After analyzing the scope and environment, the drafts are reviewed and finalized. The framework leverages domain-specific ISO standards for accuracy and compliance.

## Inside the Automation Engine

Risk assessment automation is powered by an engine containing data on threats, vulnerabilities, and risks associated with frequently used information assets. When asset information is missing from the database, GenAI retrieves it from public sources. Experts validate this data before updating the database. Key steps include:

### Asset Categorization

Based on domain standards (e.g., ISO 14971 for healthcare, ISO 21434 for automotive).

1

### Threat and Risk Generation

The dynamically maps threats and vulnerabilities to asset metadata.

2

### Risk Score

Based on impact and attack feasibility, used to categorize risk levels.

3

### Control Evaluation

Existing controls are evaluated, and residual risks are identified.

4

### Remediation Recommendations

Risk treatment options and additional control suggestions are provided.

5

### Stakeholder Updates

Risk owners are notified of assessment outcomes.

6

### Report Generation

Customized reports in formats aligned with ISO standards and other industry standards.

7

### Continuous Learning

The system dynamically updates itself with new asset data using GenAI.

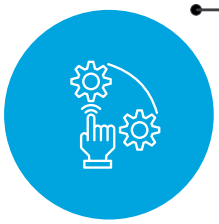
8

## Business Benefits/ Best Practices

Cyient's CySecAssure simplifies risk assessments across domains like automotive and healthcare. It enables:

### Faster Compliance

Supports standards like ISO 21434, ISO 27001 for regulations such as UN R155/R156.



### Automated TARA

Covers in-vehicle, out-vehicle, and network-level assessments.

### Identifies Threats, Vulnerabilities and & Risk Visibility

Proactively identifies vulnerabilities and security gaps.

### Asset Protection

By assessing risks, organizations can Helps prioritize critical assets for effective mitigation.

### Informed Decisions

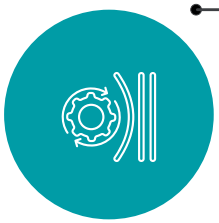
Offers data-driven insights for security planning and investment.

### Reduced Risk Exposure

Minimizes chances of breaches and costly penalties.

### Reputation Safeguarding

Demonstrates diligence in protecting user's and enterprise's sensitive data.



### Resilience Building

Enables quicker response to operational disruptions.

## Case Studies

### TARA for a Global Automotive OEM

Cyient conducted TARA (Threat Analysis and Risk Assessment ) on an OEM's network infrastructure and assets including plant networks, data centers, product management applications , and engineering systems. Using the automation engine, the draft report was generated quickly and finalized with minimal effort. The overall timeline was cut from 15 months to 6 months using CySecAssure.

### Cloud-Based Application Risk Assessment

Risk assessment for an AWS-hosted enterprise application involved comprehensive vulnerability scanning, penetration testing, and remediation validation. Conducted in alignment with ISO 27001 standards, all critical and high-risk findings were addressed. Final reports were completed after iterative reviews, streamlined through CySecAssure.

### End – to -End Cybersecurity for an Asian Automotive OEM

Vehicle-level TARA was conducted to derive security goals and security requirements. The scope also included support for security library development and integration, cybersecurity validation and penetration testing, Post-Development (production and security operations), homologation for statutory compliance, and incident and vulnerability management. The reports were generated in customer-preferred templates and submitted for UN R155/R156 certification using ISO 21434.

## THE CYIENT THOUGHT BOARD

**What is the main advantage of the risk assessment automation?**

It reduces manual effort by 50%, eliminates redundancy, and minimizes human error.

**What sets Cyient's solution apart?**

It supports multiple industry standards (ISO 27001, ISO 21434, etc.) and allows customized report formats.

**How accurate is the automated assessment?**

100% accuracy when the engine uses database-sourced input data.

**What if an asset isn't in the database?**

GenAI fetches asset data from public sources, and experts validate it before inclusion.

**What inputs are input?**

A structured asset list is provided to the framework.

## Conclusion

The Risk Assessment Automation Framework enables efficient, standardized, and compliant risk assessments. By minimizing manual tasks and streamlining report generation, it ensures faster turnaround and improved accuracy. Automation is critical to meeting evolving cybersecurity and regulatory requirements.

## About the Author

**Sreelekshmi PS**
Senior Software Engineer, Cybersecurity team, Digital & Technology Group

She is a cybersecurity professional with an M.Tech in Cyber Forensics & Information Security and close to seven years of experience in the field. As a Certified Information Security Manager (CISM) and ISO 27001 Lead Auditor, she has built deep expertise in vulnerability assessments and penetration testing (VAPT), risk assessment, threat modeling, threat analysis, application security, cloud security assessment, and security audits across a wide range of products, services, and domains. Her strong foundation in Governance, Risk, and Compliance (GRC), along with hands-on experience in data privacy implementation, enables her to drive security strategies that are both effective and compliant. Sreelekshmi is well-versed in global standards and regulatory frameworks, including ISO 27001, ISO 21434, GDPR, DPDPA, CCPA, HIPAA, CSA STAR certification, as well as NIST, COBIT, ENISA, SOCI, CRA, and the EU AI Act. With a keen eye for emerging threats and a commitment to continuous learning, she consistently delivers cybersecurity solutions that support business resilience and regulatory alignment.

## About Cyient

Cyient (Estd: 1991, NSE: CYIENT) delivers intelligent engineering solutions across products, plants, and networks for over 300 global customers, including 30% of the top 100 global innovators. As a company, Cyient is committed to designing a culturally inclusive, socially responsible, and environmentally sustainable tomorrow together with our stakeholders.

For more information, please visit www.cyient.com

## Contact Us


### North America Headquarters
Cyient, Inc.
99 East River Drive
5th Floor
East Hartford, CT 06108
USA
T: +1 860 528 5430
F: +1 860 528 5873

### Europe, Middle East, and Africa Headquarters
Cyient Europe Limited
Apex, Forbury Road,
Reading
RG1 1AX
UK
T: +44 118 3043720

### Asia Pacific Headquarters
Cyient Limited
L14, 333, Collins Street
Melbourne, Victoria, 3000
Australia
T: +61 4 7026 3817
F: +61 3 8601 1180

### Global Headquarters
Cyient Limited
Plot No. 11
Software Units Layout
Infocity, Madhapur
Hyderabad - 500081
India
T: +91 40 6764 1000
F: +91 40 2311 0352


Follow us on: