



# Platform X

## Cyber Risk Management Solution

Cyber Risk Management made simple and easy to monitor

Platform X – IT Security and Vulnerability Management is a holistic and widespread solution that helps in organizations to consolidate Vulnerabilities on their IT assets leverage the inbuilt Rule Engine for Exception relation decision making and recording observations/Findings. The application helps organizations to identify vulnerabilities on the Hardware and Cloud based assets and segregate it based on a rule engine and take appropriate actions and create detailed reporting and enable Cyber Admins to create Self-Identified Risks.

### Advantages



#### Cyber Risk Program Streamlined

Businesses can leverage Platform X – IT Security and Vulnerability Management to streamline the Cyber Program and prioritize critical IT Asset from Vulnerability standpoint



#### Asset Prioritization as per Business Functions

The Vulnerability Postures can be generated for different Business Functions for there related Assets



#### Recover more quickly

Through Vulnerability scan results and Business User understandable reports will help Admins to take decisions for Critical/High Business Assets from Business Continuity Standpoint.



#### Governance Data Management

Cyber Professions can manage the orphan Assets and Risk Identified and create mapping and provide relationships.

# Capabilities

## ▪ Vulnerability Scan result Consolidation

Cyber Program Managers can create Assets in the Governance library. Pull vulnerabilities from Asset scanners and consolidate and mark the Vulnerabilities based on the criticality.

## ▪ Rule Engine

Seamless Rule Engine can be used to define the key decisions which system can help user to take on Vulnerabilities. Rule Engine can be used to designate Vulnerabilities to mark with an Exceptions, create Issues or mark the scan result as false positive.

## ▪ End to End Automation

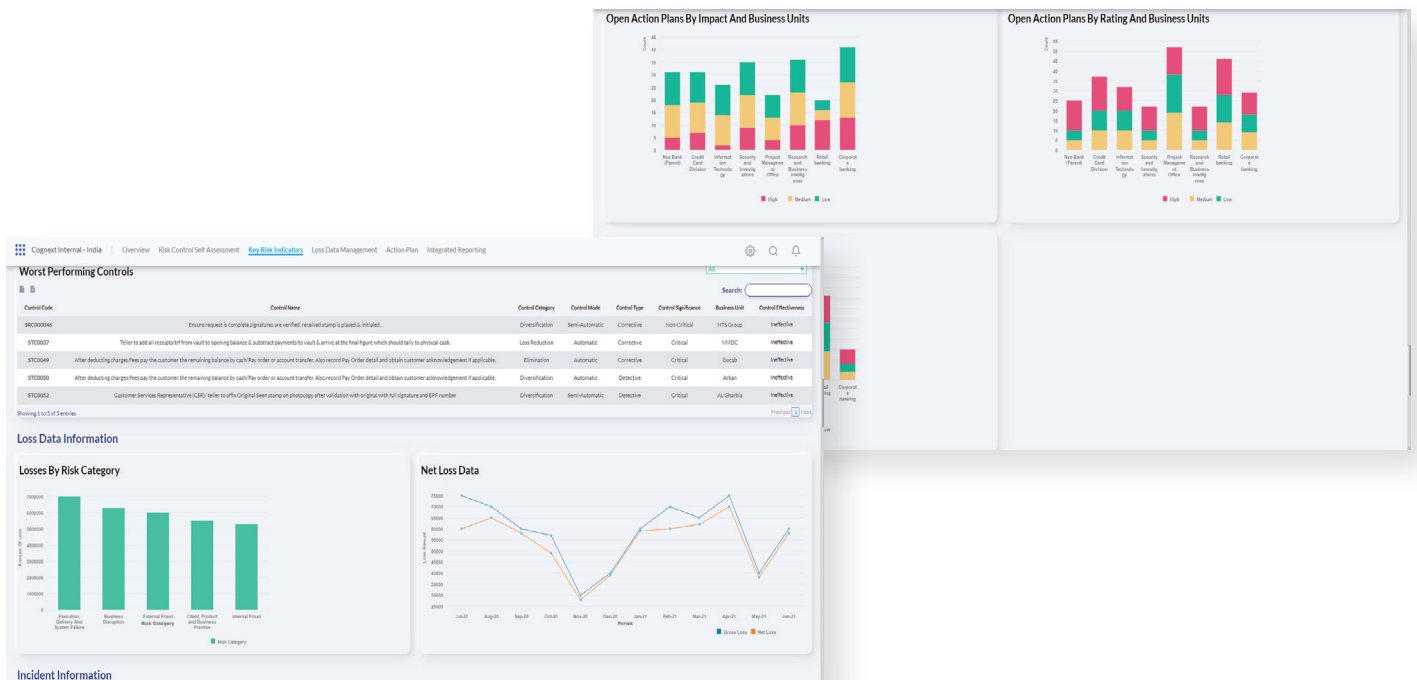
The entire workflow including the identification of Vulnerabilities and passing it to library and report generation for scan results. The highly tensible Rule Engine adds immense value to the automation as the vulnerabilities can be flagged in case false alarm or marked with an exception or triggered an Issue

## ▪ Action Plan and Mitigation

Action Plan and Mitigation component can be leveraged for managing all the Issues triggered for the Vulnerabilities. The Action Plans will be automatically raised based on configurable templates. The triggered Action Plans will be monitored through list reports and interactive dashboards

## ▪ Reporting and Dashboard

Inbuilt business intelligence layer that provides unified graphical and responsive dashboards, intelligent and actionable reports for efficient management decisions. Enables analyzing critical information from Vulnerability standpoint and enable user to take decisions for self-identified risks and orphan Assets.



CONTACT US | REQUEST A DEMO

Email: [info@cognext.ai](mailto:info@cognext.ai)

[www.cognext.ai](http://www.cognext.ai)

[www.linkedin.com/company/cognext-ai](https://www.linkedin.com/company/cognext-ai)

cognext