Unified GRC Platform

Audit Module

The Problem Statement

- Siloed departments: Governance, Risk, Compliance, and Audit operate independently
- Fragmented tools and duplicated efforts
- Delayed insights and non-actionable risk intelligence
- Missed regulatory mapping and audit gaps
- Lack of KRI ‘s in driving the Risk based Audit Methodology
- Absence of a structured process for anticipating and assessing both external and internal threat scenarios, resulting in inadequate cyber risk forecasting and limited organizational preparedness.
- Lack of Single Source of Truth

Our Vision

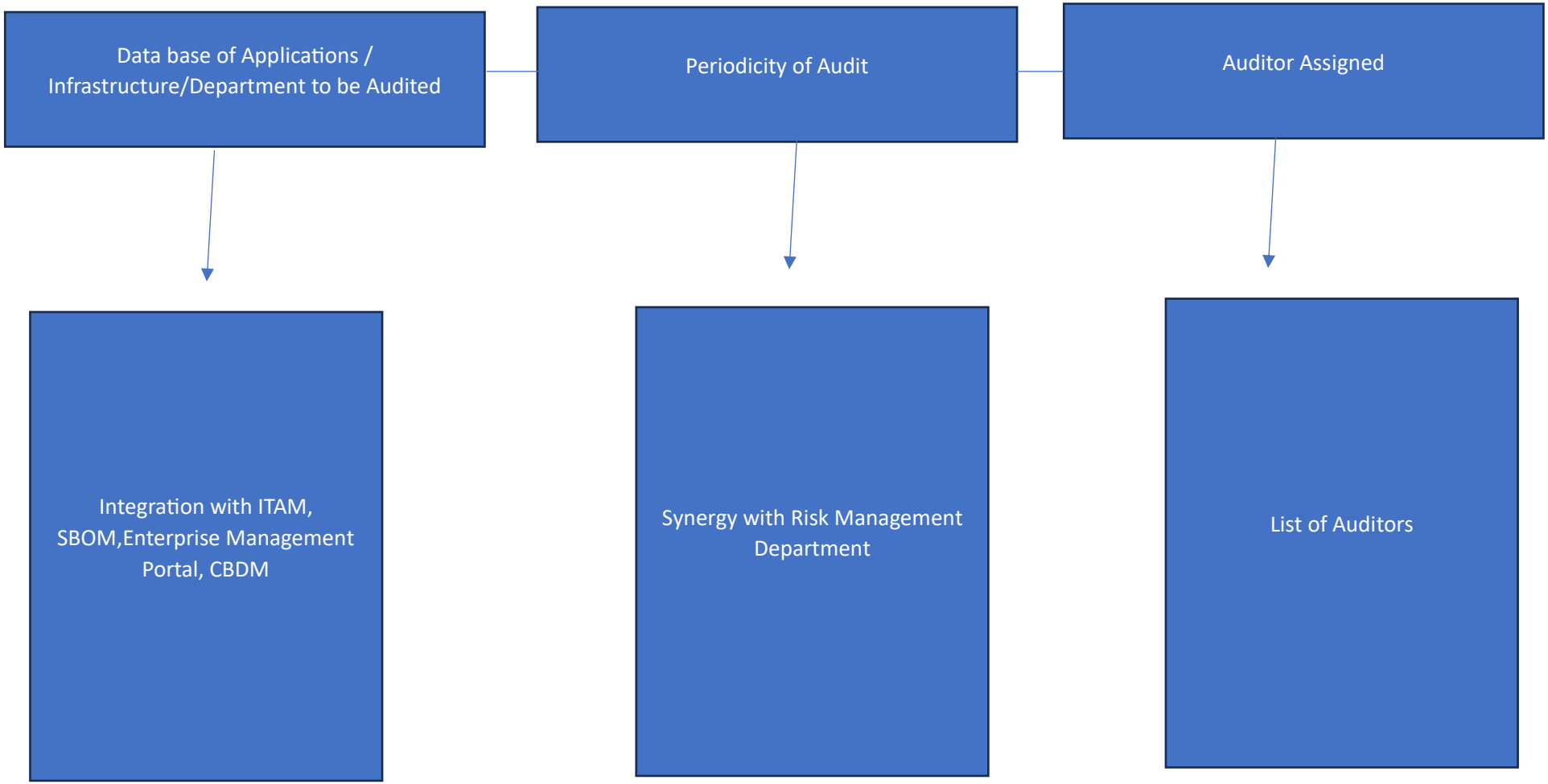
- One platform for Governance, Risk, Compliance, and Audit
- Foster effective synergy and collaboration among the First, Second, and Third Lines of Défense, including the integration and coordinated use of tools managed by each line, to enable intelligence-driven decision-making across the organization.
- Centralized Platform that integrates with Cyber security tools (SIEM , SOAR, EDR,DAM etc), Centralized dashboard(Antivirus, Patch Management)
- Centralize Platform standardize, and govern security-related information such as asset inventories, user identities, incident logs, and configuration baselines—within an authoritative, auditable repository.
- Centralize Platform that integrates with various Risk assessment activities that includes Comprehensive risk assessments, Vulnerability assessment , Penetration testing etc.
- Centralized platform or data lake that consolidates frameworks, policies, and guidelines issued by regulatory bodies such as the RBI, SEBI, NCIPPC, ISO 27001, NIST, and DPDP, along with the organization's own policies and frameworks.
- Delivering required KPI’s for implementation of Risk Based Audit

Key Capabilities

- Synergy across departments: seamless input/output flow
- Dynamic risk scoring from audits.
- Audit-aware risk models incorporating past insights
- Automated control mapping with SOPs and frameworks
- Smart Audit Assistant for control suggestions
- Recurring issue tracking and classification
- Activity-wise compliance scoring and dashboards

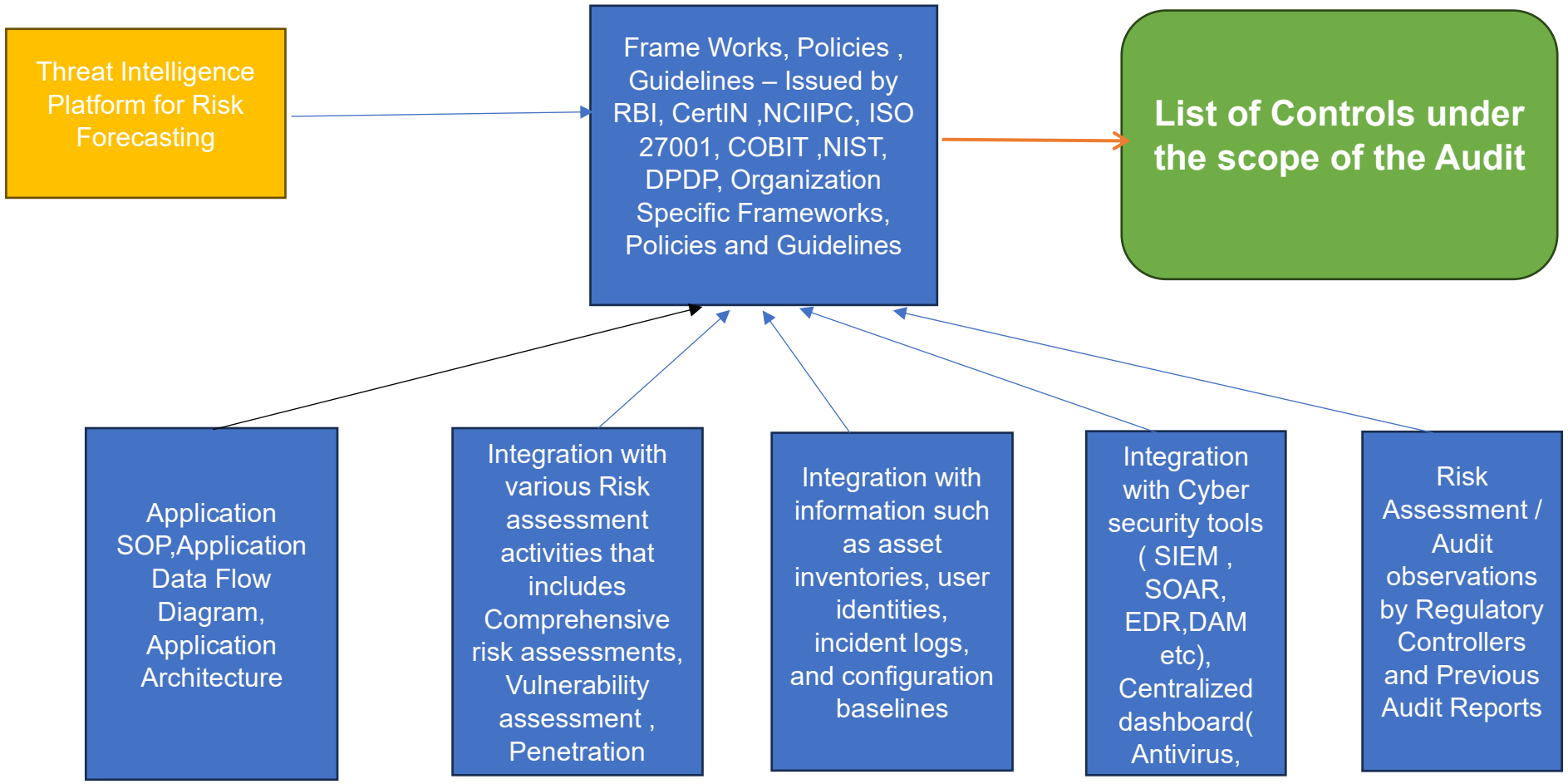
Application Architecture

1. **Audit Plan Automation(Audit -> When and What to do)**



2. Defining the Audit Scope - Automation

- Controls to be audited – For a particular Application or Infrastructure is being derived automatically ,



3. Observation Intelligence & Compliance Scoring

- Auto-classifies observations: Access, Backup, DR, Change Mgmt, etc.
- Aggregates audit results to score compliance activity-wise
- Identifies persistent weaknesses and recurring issues
- Auto Risk assignment : Each Observation is assigned with particular category of risk and allocation weightage for the same, Sample Parameters considered for assigning the risk
    - Impact of the Observation
        - Human Loss
        - Financial Loss
        - Reputational Loss etc
    - Persistent in Nature
    - Criticality of the control etc

4.Knowledge Database Enablement - Observations

Intelligent GRC Repository

- Central library with:
    - All closed/open observations
    - Mapping to controls and frameworks
    - Root cause categories
    - Action taken + effectiveness rating

AI-Powered Search

- “Has this issue occurred before in any other unit?”
- “What was the last control audit checklist for ISO 27001 A.12.4?”
- “Give me examples of successful DLP non-compliance closures.”

Learning Loop

- Tool tags patterns in:
    - Most common failure domains (e.g., patching, access)
    - Longest time-to-close categories
    - Policy violations not covered in any audit

5. **Reporting & Dashboard Capabilities**

1. Application-Wise / Department-Wise Audit Reports

- **Cross-functional Context:** Audit reports integrate insights from Risk, Compliance, SOC, and Governance teams.
- **Criticality-Aware Scoring:** Each application's score is weighted by business impact and security posture.
- **Auto-Mapped Controls:** Control lists auto-tagged with relevant ISO, NIST, RBI, SEBI, and CERT-In requirements.
- **Historical Trends:** Time-series visualizations showing compliance improvement or regression.

2. Trends and Forecasting

- **Predictive Analytics:** AI models forecast control failures based on historical audit, incident, and risk data.
- **Process-Wise Patterns:** Identifies process-specific weaknesses (e.g., patching fails post-change window).
- **Heat Maps and Risk Zones:** Highlights departments or applications that consistently underperform.
- **Audit Planning Engine:** Ranks future audit priorities using forecasted non-compliance likelihood.

3. Activity-Wise Reporting (Backup, Access, Incident, Change, etc.)

- **Unified View:** Consolidated reporting of control effectiveness across all activities.
- **Repeat Observation Detection:** Detects recurring control failures across systems or time periods.
- **Activity Health Scoring:** Assigns maturity levels to each control domain based on issue density.
- **Custom Filtering:** Drill-down by department, control type, observation severity, or control owner.

4. Centralized Visibility for Top Management

- **Application Level:** Real-time audit readiness, control gaps, and regulatory risk exposure.
- **Department Level:** Overview of compliance maturity, audit findings, and closure timelines.
- **Activity Level:** Insight into cross-departmental control domains (e.g., Backup, Access, Change).
- **Risk-Based Level:** Visibility into top organizational risks aligned with audit and incident data.
- **Framework Level:** Dashboards showing coverage and gaps per framework (ISO, NIST, RBI, etc.).

5. Single Source of Truth (SSOT)

- **Live Integration:** Syncs with ITAM, SBOM, SOC tools (SIEM, EDR), asset registry, change logs.
- **Unified Control Inventory:** One master list of all controls mapped to regulatory and org needs.
- **De-Duplicated Observations:** Ensures one consistent view of every issue across GRC modules.
- **Traceability:** Track each observation from origin to closure with linked policies, SOPs, evidence.
- **CXO Dashboard:** Executive-level summary with drill-down options and risk-weighted insights.

Strategic Benefits

- **Reduced Audit Fatigue:** Meaningful, context-aware audits reduce redundancy.
- **Continuous Compliance:** Near real-time compliance visibility for internal and external frameworks.
- **Risk-Aware Decision Making:** Leadership sees not just non-compliance, but its impact.
- **Improved Accountability:** Every observation and control is mapped to responsible owners.
- **Faster Remediation:** Knowledge database assists in fixing issues using past resolution patterns.

Glimpses of Synergy with other department

1.**Risk Management Department through Synergy** □ The unified tool enhances risk assessment capabilities by leveraging cross-departmental intelligence. Governance frameworks define baseline expectations, while audit and compliance modules enrich risk context:

- Audit Module Insights: Real-time feed of audit findings, severity levels, and control compliance scores directly influence the application's risk profile.
- Compliance Scoring: Deviations from mandated controls and standards are automatically flagged, contributing to the dynamic risk posture.
- Risk Weightage Calibration: Governance policies guide how observations are weighted in risk scoring — factoring in recurrence, regulatory mapping, and business criticality.
- Synergized Outcome: Risk scoring becomes multi-dimensional — integrating policy alignment, control performance, audit results, and compliance maturity — enabling smarter prioritization and informed mitigation planning.** Produces a calibrated, context-rich application risk rating that reflects both compliance posture and audit history**.**

2.Compliance Tracking Through Synergy

- **Automated Ownership & Accountability:** Assigns observation owners and remediation timelines dynamically based on issue type, severity, and business impact (e.g., Infra → IT Ops, DR → BCM Team).
- **Smart Escalation Engine:** Flags overdue, high-risk, or repeat findings and notifies responsible teams and management.
- **Intelligent Remediation Suggestions:** Recommends closure actions using historical resolution data and links to a centralized knowledge base of proven fixes.
- **Integrated Workflow & Evidence Tracker:** Tracks the status of remediation tasks, maintains audit trails, and supports evidence uploads for closure validation.

- **Cross-Functional Visibility:** All stakeholders can view status, dependencies, and blockers in real time, ensuring transparency and collaboration.