Cheat sheet

GRC – Governance, Risk & Compliance

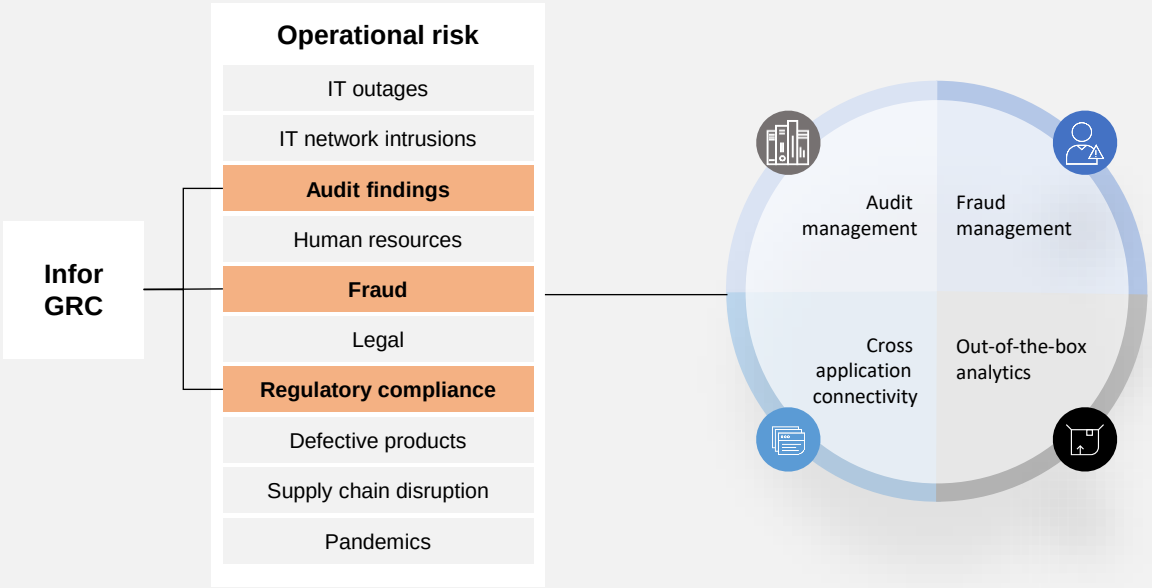
Key concepts and definitions

GRC (Governance Risk & Compliance)	GRC (Governance, Risk, and Compliance) is a process used to ensure that organizations manage their business in accordance with regulatory requirements and meet their internal objectives for risk management, operations, and performance.
Governance	The process of implementing policies and ensuring that they are executed.
Risk	The process of reducing risk and uncertainty through the establishment of business objective and governance mechanisms.
Compliance	Adhering to the business rules, policies and guidelines whether they are internally or externally implemented.
Application Instance	The connections between the Infor GRC application and the Data lake.
Insights	Include the definition to classify the data to be monitored in an application.
Tasks	An execution of a process in the Infor GRC application.
Schedule	The functionality in the GRC application to analyze data and the certification process.
Provision	A request raised for the User Provisioning. A provision can include a user creation or modifying the access for a user.
Rule Book	A collection or group of rules.
Rules	Include one or more conditions to identify risks in a business process.
Conditions	A definition of a business process or a business activity. The conditions are the part of a rule.
Violations	Violations are generated when data from an application is analyzed based on the predefined conditions in a rule.
Mitigation	The Infor GRC function that enables the user to resolve the violations.
Compensating Control	Documents that contain the business justification, the processes or agreements that are used for mitigating rule violations.
Approval Process Template	Consolidates the stages and the approval process conditions to define an approval process.

Resources

Product Overview | YouTube | Documentation | Education | Dev Portal | User Community

GRC Risk Address and Highlights



Infor GRC Capabilities

Authorizations Insight	Access Manager & Emergency Access	Certification Manager	Process Insight
Segregation of duties(SOD) • FSM & HCM • Identify access conflicts inherent to or across systems • Insightful security & violation reporting • Document mitigating controls to facilitate closed loop remediation • What-if simulations for test access changes	**Compliant User Provisioning** • Prevent control & compliance issues • Streamline security change management • Advanced Approval Process • Audit trail of all activities • Emergency Access/Fire Fighter access for minutes or a day	**Periodic access review & verification** • Review of user's system accesses for appropriateness • Enforce periodic & consistent review process • Option to automatically revoke rejected access • Retain history / audit trail of all past actions	**Identify financial risks & non-compliance** • Monitor business transactions and master data for anomalies • Wide Business Controls Coverage • Monitor regulatory Watchlists(e.g. OFAC to identify bad actors in customer/ vendor master
Audit findings/SOX concerns	**Change management**	**User attestation**	**Fraud concerns**