

GRC Tool Evaluation for Healthcare Compliance

Executive Summary

I developed a strategic framework for selecting GRC tools aligned with the organization's regulatory and operational needs. I identified scalable GRC solutions that strengthened compliance, safeguard patient data, and support long-term healthcare innovation.

Organizational Profile

A major U.S. healthcare provider offering hospital based care, outpatient services, and telehealth solutions. The hospital manages significant volumes of sensitive health data and must comply with a complex network of healthcare regulations and standards.

Selection Criteria and Recommendations

During GRC vendors evaluation, the following capabilities were prioritized:

- Healthcare specific compliance modules (HIPAA, HITECH, CMS)
- System integration with EHR platforms (e.g., Epic, Cerner)
- Automated incident management and reporting
- Role-based access and audit controls
- Proven scalability and vendor support in the healthcare industry
- Workflow automation for claims processing.

Recommended vendors for evaluation:

- **NAVEX** – Comprehensive compliance management tailored to healthcare
- **LogicGate** – Flexible GRC workflows and strong risk visualization
- **OneTrust** – Strong privacy and data governance capabilities
- **RSA Archer** – Mature platform with dedicated healthcare modules
- **SAI360** - EHR and PHI risk tracking, prebuilt healthcare compliance content.
- **Onspring Healthcare Compliance Suite** - Automates billing/coding compliance, policy lifecycle, and healthcare audits.

Conclusion

I identified and recommended GRC tools that align with the hospital's regulatory and operational needs. The selected solutions support HIPAA compliance, enhance EHR governance, strengthen data security, and streamline claims oversight, positioning the organization for improved risk management and long-term compliance success.