How to measure return on investment in RSA Archer implementations

Return on investment (ROI) is a common financial metric used to evaluate the value derived from an investment to determine where and how an organization is spending their resources. It often forms the basis for initial or follow-up decisions to implement GRC programs on RSA Archer, and as such, needs to be a critical part of your planning and execution model.

For GRC implementations, common metrics used to measure ROI are:

- Product licenses
- Professional services for tool implementations
- Ongoing tool administration
- Training and awareness
- Savings through operational efficiencies
- Labor cost savings
- Regulatory savings
- Legacy tools savings.

Measuring effectiveness of GRC implementation

GRC Implementations can be measured using the following metrics:

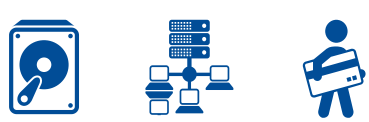
Financial metrics
Deliver detailed visibility into the financial impacts of changes to the enterprise risk and compliance posture

People
Reduced manually intense labor requirements aligning workforce towards forward looking initiatives

Process
Risk reduction leading to reduced penalties incurred due to noncompliance

Technology
Reduce costs by eliminating multiple siloed tools:

- Licensing costs
- Infrastructure costs
- Process administration tools

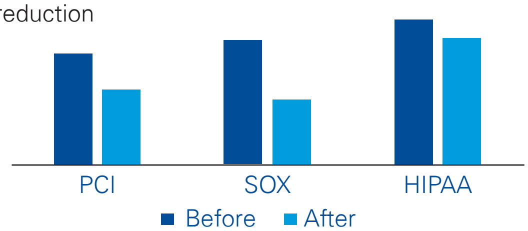


*The above charts are examples only.

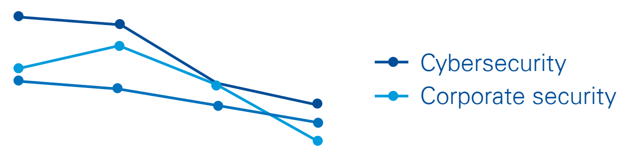
Operational effectiveness metrics

Demonstrate improved efficiency, convergence, and consistency through elimination of redundancies and errors

Percentage reduction in **audit findings** across different compliance programs due to risk reduction



Percentage reduction in **incidents** due to early identification of risks



Percentage reduction in time to manage various governance, risk, and compliance functions: Issues, Vendors, Incidents, Reporting

Qualitative metrics

Deliver detailed visibility into the financial impacts of changes to the enterprise risk and compliance posture

Consistency: Established a single system of record with common taxonomy, guiding principles, and centralizing business processes

Collaboration: Eliminated silos and fostered collaboration across different business groups

Customer satisfaction: Enabled users through simplified processes and enhanced user experience

Business agility: Facilitated the ability to make better strategic decisions using risk and compliance information

Maturity: Improved overall maturity in compliance programs through clearer alignment with industry standards

Visibility: Empowered executives with real-time reporting to raise visibility of overall risk, compliance, and security posture

*The above charts are examples only.

Key considerations

— Evaluate the ROI on a reoccurring basis before, throughout, and after the program implementation by collecting customer feedback and analyzing predefined KPIs.

— Make cost and benefit projections at least three years out to come up with benefits that are comparable to costs to build a well-rounded long-term business case.

— Baseline projected savings considering organizational culture and how quickly the end users can adopt new programs and solutions.

— Identify champions that use and promote system adoption and will serve as a valuable feedback loop.

— Don't overlook the strategic costs to guide the organizational roles and responsibilities, training and awareness, process improvements, and other elements that are critical for a successful GRC implementation.

— Don't lose focus on the vision of what GRC can offer to your organization over time.

Contact us

Lokesh Ramani
Managing Director, Cyber Security
T: 206-913-4491
E: lramani@kpmg.com

Juliet Hodder
Alliance Director
T: 510-378-6765
E: juliethodder@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia