SaltyCloud Isora

Enabling Risk, Compliance & Control Assessments

SOLUTION**PERSPECTIVE**

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

SaltyCloud Isora
Enabling Risk, Compliance & Control Assessments

Growing Demand for Assessments

Organizations operate in a complex environment of risk, compliance requirements, and vulnerabilities that interweave through departments, functions, processes, technologies, roles, and relationships. What may seem as an insignificant risk in one area can have a profound impact on other risks and cause compliance issues. Understanding and managing governance, risk management, and compliance (GRC) in today's environment require a new paradigm in managing these interconnections and relationships through a common approach to conducting assessments and managing risk. This is true in both traditional organizational environments, as well as the new era of cloud environments in which there is shared responsibility for security, risk, compliance, and control between the organization and the cloud hosting environment. It is also needed across business relationships in the extended enterprise as organizations have to assess risk and compliance in third parties such as vendors, suppliers, contractors, outsourcers, service providers, and more.

GRC departments are scrambling to keep up with multiple initiatives that demand greater oversight of risk and compliance across the organization and its relationships. Most organizations approach these issues reactively — putting out fires of security, risk, and compliance wherever the flames are hottest. As these pressures mount, GRC teams often fail to think strategically as it is too busy reacting to issues. Organizations need to step back and think strategically; to figure out how to streamline resources and use technology efficiently, effectively, and agilely to manage and monitor assessments across their environment.

A reactive approach to risk and compliance assessments is not sustainable in an environment of growing pressures, and is a recipe for disaster that leads to:

Higher cost, from . . .

- **Wasted and/or inefficient use of resources.** Silos of reaction to risk and compliance needs and issues lead to wasted resources. Instead of leveraging assessments and resources to meet a range of risks and compliance requirements, assessments are developed haphazardly in documents, spreadsheets, and emails that take a lot of time to manage. Organizations often try to relieve the symptoms instead of thinking how to address the root cause. GRC teams end up with different internal assessment processes, systems, and documents/spreadsheets 'in play' to meet individual risk and compliance needs.

- **Unnecessary complexity.** Multiple risk and compliance approaches introduce complexity which in turn adds overhead costs and increases inherent risk. Assessments are impossible to streamline and manage consistently, introducing more opportunities for risk and compliance to fail or go unmonitored. Inconsistent assessment processes also produce inconsistent documentation, which further confuses security, regulators, and the line of business.

Inability to align with the organization, resulting in . . .

- **Lack of agility.** Complexity drives inflexibility. Manual document-centric assessment become so wrapped up in spinning individual risk and compliance assessments and reacting to them that support of the business is degraded. GRC staff, along with the business, is bewildered by a maze of varying documents and approaches that are not designed with any consistency or logic, and struggle to apply and assess this in today's modern business and cloud environments.

- **Vulnerability and exposure.** A reactive approach leads to more exposure and vulnerability. Complexity means departments are focused on their own silo of risk, and no one sees the big picture across assessments and the interconnections of risks and controls. No one looks at risk and compliance exposure holistically or contextually, with regard for what is good for the business in the long run. Varying and independent manual assessment efforts around the organization and cloud lead to difficulty demonstrating control with a result in confusing audits and assessments.

Not only does a reactive manual and document-centric approach to assessments lead to greater vulnerability and exposure, it also means higher costs for the organization. Addressing risk, security, compliance, and control across a series of disconnected projects and assessments leads to inefficiency in management and operations, wasted spending on redundant approaches, and a greater burden to the business.

The bottom line: When organizations approach security, compliance, and control in scattered documents and disconnected processes there is no possibility to be intelligent about risk and compliance decisions that impact the broader organization, its operations, and adherence to regulations and standards. Organizations need an integrated assessment architecture that delivers 360° contextual intelligence on assessments for risk, compliance, security, and control.

SaltyCloud Isora

Enabling Risk, Compliance & Control Assessments

SaltyCloud Isora is a solution that GRC 20/20 has researched and evaluated, that can manage risk, compliance, and control assessments in complex, distributed, and dynamic organizations environments, this includes assessments of third-party relationships. Isora delivers an integrated assessment platform that can be used to manage, deliver, and report on the range of risk, compliance, and control assessments to a range frameworks, standards, and regulations.

GRC 20/20 finds that the Isora solution enables organizations to be efficient, effective, and agile in their GRC related assessment management strategy and processes for both the traditional organizational environment, as well as third party relationships. Isora is well suited for use across industries and organizations from small to large to manage the range of risk and compliance assessments that are being conducted.

GRC 20/20's evaluation of Isora reveals that it:

- **Automates** risk, compliance, and control assessment processes

- **Provides** an intuitive and easy to use interface

- **Documents** controls and requirements to satisfy regulators and stakeholders

Isora simplifies and strengthens risk, compliance, and control processes in organizations. It is particularly well adept to meet the needs of the small to mid-market but can be used across industries. The SaltyCloud solution has shown specific traction in the higher education market.

GRC 20/20's evaluation, research, and interactions with SaltyCloud clients has determined the following:

- **Before SaltyCloud Isora.** Clients of Isora typically are replacing manual processes of risk, compliance, and control assessment that are encumbered by documents, spreadsheets, and emails. Such approaches can be very manual, time-consuming, and prone to errors -particularly in aggregation and reporting on data that involves hundreds to thousands of documents and spreadsheets. Some clients came from complicated GRC platforms where the cost of ownership to maintain the solution was too much and they needed something more agile.

- **Why SaltyCloud Isora.** Organizations choose Isora as they are looking for a single integrated information architecture to automate and manage risk, internal control, security, third party, and compliance assessments. Clients were looking for a single information architecture that can handle an integrated taxonomy of assessments that is agile and intuitive. Clients state they chose Isora as the capabilities of the solution met their needs, but it presented a lower cost of ownership – from acquisition through maintenance – over competitors. Organizations specifically valued their proven success in academic environments, minimal initial configuration, satisfaction with other SaltyCloud products, and low cost of ownership.

- **How SaltyCloud Isora is used.** Typical use cases for Isora vary to meet a variety of assessment challenges, such as a single regulatory requirement, to cross-department integrated approaches to risk, compliance, and control assessment. These include:

  - Internal control assessment

> Application security assessments

> Vendor risk assessments

> IT risk assessments

> Standards and regulatory compliance (e.g., NIST 800, CSF)

> Security assessments for cloud providers

■ **Where SaltyCloud Isora has excelled.** Organizations state that Isora has improved the quality of their assessment information, reporting, and processes. This improves the organization's overall visibility into GRC contexts across the organization, while eliminating the overhead of managing manual assessment processes encumbered by hundreds to thousands of spreadsheets, documents, and emails. Clients find that the solution is flexible to adapt to their requirements, has the core capabilities needed, and provides them the ability to grow and mature their program over time. Overall, users find the solution was particularly easy to implement and rollout in their organization.

What SaltyCloud Isora Does

GRC 20/20 has evaluated the capabilities of the SaltyCloud Isora solution and finds that it delivers an intuitive and robust assessment management solution to manage the range of risk, compliance, and controls assessments in both traditional on-premises and third-party vendor environments, in context of today's demanding requirements and dynamic environments. Isora automates what were once labor-intensive tasks associated with managing risk and compliance assessments. This functionality is essential for eliminating a maze of manual processes, documents, spreadsheets, email, and narrow point solutions.

SaltyCloud Isora Enables the GRC Assessment Lifecycle

SaltyCloud Isora effectively and efficiently enables an organization's end-to-end assessment management strategy by providing a platform to manage the lifecycle of assessments across the organization and its environments. This lifecycle that Isora automates, includes:

■ **Defining scope and requirements for assessments.** Isora provides a framework of control for compliance and risk assessments. This supports adherence and compliance to a range of regulations and standards, such as NIST standards, ISO 27000, and more. Organizations can also add their own specific assessment requirements in context of the framework provided.

■ **Assessment.** Utilizing the scope of requirements, the organization can then do the initial assessment of their organization or system against the requirements to validate and document compliance and control.

GRC ASSESSMENT LIFECYCLE

- **Ongoing continuous monitoring.** Assessment is not a one-time effort with Isora, it is something that can be regularly scheduled or triggered when events happen. Isora can be used to regularly manage and reassess the environment to ensure they are always compliant and risk is mitigated. This is critical in today's dynamic technology and business environments.

- **Remediation.** When issues are discovered, Isora is used to define workflow and tasks to ensure they are remediated.

- **Documentation & reporting.** Isora streamlines the documentation and reporting on cloud control and compliance. This saves significant time for staff that had to manually reconcile and validate controls and assessments done in scattered processes, documents, and emails.

04 CONTINUOUS MONITORING

03 BROADEN SCOPE

02 REMEDIATION

01 ASSESSMENTS

ANALYSIS

DOCUMENTATION
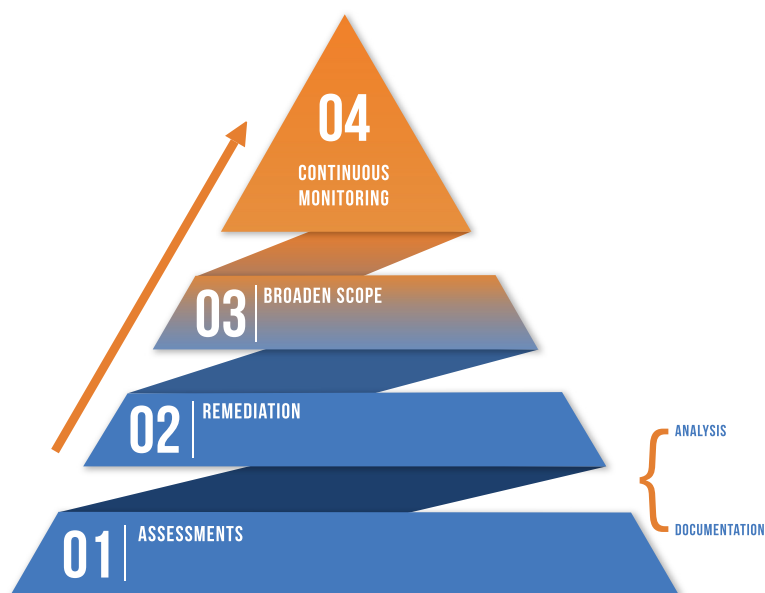
Foundational Capabilities in SaltyCloud Isora

While SaltyCloud Isora can manage be used for managing assessments across the range of internal processes and systems that organizations have. Specific capabilities Isora delivers that enable organizations in managing assessments, no matter the scope, are:

- **Configurability.** Isora is designed to be adaptable to the unique requirements of organizations. The solution is able to evolve to accommodate the dynamic nature of assessments, as well as changing business and regulatory requirements.

- **Content integration.** Isora has integrated and mapped an array of frameworks, regulations, and standards for controls so organizations can assess once and comply with many.

- **Analytics.** Isora delivers assessment analytics that are intelligent through the triangulation of collected information across systems and initiates remediation tasks when needed.

- **Notifications.** Isora provides notification through emails to notify stakeholders and others of programs and expectations with embedded links to assessment questionnaires and tasks.

- **Workflow and task management.** The Isora solution provides a full range of capabilities to flexibly manage workflow and tasks. This includes alerts on pending tasks that are soon due and escalation of missed tasks.

- **Questionnaires, self-assessments, and surveys.** The Isora solution delivers a full range of assessment survey capabilities to gather information from stakeholders with embedded instructions and validations to help ensure completeness and accuracy.

Benefits Organizations Can Expect with SaltyCloud Isora

Organizations are most likely to move to the SaltyCloud Isora platform because they found that their manual document-centric approaches took too many resources to administer, only addressed specific areas of control, and found things slipping through the cracks because of the continuous barrage of change. Some organizations choose Isora because their existing GRC management platform was too complex or was too costly in the complexity, licensing, and administration of the system.

Specific benefits organizations can expect from implementing the Isora solution are:

- *Significant efficiencies in time* through automation of workflow and tasks, as well as reporting. Specifically, the time it took to build reports from documents and spreadsheets now is just a matter of seconds.

- *Reduction in errors* by automating the validation of compliance and controls - removing errors from manual processes and reconciliation that was incomplete or incorrectly entered.

- *Data integrity* with Isora being the system of record for all assessment and control information.

- *Collaboration and synergies* by providing a single platform with a consistent interface to manage assessment and interactions across departments - instead of different departments doing similar things in different formats and processes.

- *Consistency and accuracy of information* as all internal stakeholders have to conform to consistent processes and information collection. A single solution with a uniformed and integrated assessment process and information architecture.

- *Accountability with full audit trails* of who did what and when; this particularly delivers value in fewer things slipping through the cracks.

Considerations in Context of SaltyCloud Isora

Every solution has its strengths and weaknesses and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of SaltyCloud Isora to enable organizations in the consistent control management and monitoring of cloud environments — readers should not see this as a complete and unquestionable endorsement of SaltyCloud or the Isora solution.

Overall, organizations should have a high degree of satisfaction with their use and implementation of Isora as an assessment platform to manage the array of risk, compliance, and control assessments. The solution's adaptability and ease of use is of a particular benefit to organizations. The solution is agile by allowing distributed roles to get what they need while providing consistency across all involved functions.

Isora is a key piece of a broader GRC architecture. It is the piece that manages assessments that can then be used for broader risk analytics and management. Users would like to see a broader downstream capability to assign and track risks that are discovered through an assessment.

GRC 20/20 finds that Isora provides value in managing the lifecycle of assessments across departments and functions. As many organizations respond to growing regulatory requirements and risk exposure across their environment, they look for a solution like Isora to manage and automate this process.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.