7 Ways Clear Skye Enhances ServiceNow Integrated Risk Management

WHITE PAPER

ClearSkye

Reduce business risk,
preserve consumer trust,
and maintain regulatory
compliance with Clear Skye.
Natively built on ServiceNow.

Proudly built on the **Now Platform**

Built on now™

Risk Is a Business Challenge

The digital boom continues providing new and increasingly novel ways for businesses to create new business models and enrich the consumer experience. Collectively, this trend is referred to as Digital Transformation. This is great for the top line, but it can also add security and compliance risk.

As organizations evolve, an appropriate cybersecurity stance takes on added importance. In fact, managing security and risk is now firmly on the executive board's agenda – not only to open up new and innovative business solutions but also to stay out of the security breach headlines.

The Cost of Breaches and Non-Compliance

Two costs associated with unmanaged risks are non-compliance within a regulated industry, and a data breach.

According to the latest Ponemon Institute Data Breach report, the global average total cost of addressing a data breach has been rising over time and is currently $3.86 million. The United States tops the list with an average cost of $8.64 million.

Along with the need to prevent breaches from happening, most organizations must comply with one or more regulatory statutes intended to protect customers, employees, and investors from the risk of data breaches. Fines for non-compliance with regulations like SOX, HIPAA and GDPR continue to rise as well, with Ponemon pegging the average cost of non-compliance at $14.82 million in 2020.

Lax Permissions Provide Easy Entry

Common causes of data breaches and non-compliance findings include human error, system glitches, and malicious attacks. Ponemon's report found that cloud migration, IT complexity, and third-party involvement were cost amplifiers.

Both internal and external actors can cause a breach. A hacker may uncover a computer or application account with super-admin rights and move horizontally through an organization using these god-like access rights.

Or an employee may have incorrect IT permissions that don't relate to their job, which provides an opportunity to purposefully or mistakenly leak data. Regardless of where bad actors come from, all breaches take advantage of the entitlements or permissions found across the application stack.

Integration Risk Management (IRM) as a Critical Line of Defense

Organizations regularly turn to their risk management programs and supporting solutions to prevent data breaches and non-compliance findings. Industries, governments, and international bodies define and enforce regulations (and levy fines) to drive intended organizational behaviors. When a data breach occurs, your challenge is how to limit exposure by ensuring and proving policy compliance within your organization.

IRM programs are an increasingly popular approach to managing risk and compliance requirements. An effective IRM incorporates cross-functional processes to help an organization reduce residual risk, quickly identify and respond to risk events, and learn and further refine risk mitigation activities.

An IRM program's function is to provide overall enterprise-wide transparency into risks and issue management. A common IRM approach to creating such transparency is to develop **Governance, Risk, and Compliance (GRC)** processes that are administered across an organization. GRC enables the organization to align to corporate objectives, be proactive in risk identification, detect abnormalities quickly, and effectively respond to risk events. Doing this consistently creates visibility into overall risk posture and increases the likelihood of achieving corporate objectives.

As it relates to data breaches, one primary risk is poorly controlled access to data and supporting systems. Obviously, your control objective is to provide the right level of digital access to the right people at the right time. But why do breaches continue to happen because of poorly managed system access rights? Many times, it is because of inadequate governance processes over established controls. Establishing adequate GRC processes within the context of IRM will help an organization create effective governance processes. This enables prevention and swift detection of risk incidents and lowers the cost of achieving regulatory compliance.

The Solution: Clear Skye IGA

Providing the right access to the right people at the right time, and proving this access is correct, is a key **Identity Access Management (IAM)** discipline. **IGA** takes this one step further — linking IAM processes to policy and compliance requirements, including audit support.

This is where Clear Skye IGA can help. Clear Skye IGA supports organizational compliance natively on ServiceNow. This provides GRC Controls with continuous evidence collection relating to digital identity lifecycle events, application security permissions, and other functions related to Identity Governance, such as peer group analysis, user access reviews, and application security permission investigations.

To see how Clear Skye can help, let's first understand what IGA is and then explore how Clear Skye enhances ServiceNow's IRM solution in 8 key ways.

Introduction to IGA

IGA focuses on minimizing the inherent risk in giving permissions, or entitlements to users across an organizations systems and applications. IGA is a key component in a risk management program and provides great benefits in both security and operational efficiency within an organization. It supports the assignment of digital access rights to workers during their employee journey as they join, move through, and leave an organization. IGA provides automatic and requestable means of assignment of IT permissions to all types of workers, internal or external, regardless of type.

IGA solutions come in many shapes and sizes, but there is a commonly accepted set of expected capabilities.

Identity Lifecycle Management This set of capabilities is used to automate the assignment of application permissions as knowledge workers join the company, switch roles, and eventually leave the organization.

Access Request Even the most robust lifecycle management policies won't be able to automate access to everything users need to do their jobs. Access request capabilities provide a simple interface to request access and, pending the appropriate approvals, fulfil the requested access.

Access Review Regulations, as well as security best practices, require the regular review of who has what access across the application estate. Access review capabilities automate these events and provide an audited record of confirmation or denial of assigned entitlements.

Compliance Reporting and Dashboards Organizations must provide auditors with reliable and accurate information on access to data and applications. IGA solutions typically provide organized and detailed reports that show every entitlement change, along with who authorized it.

Regulatory Drivers for IGA

IGA programs are a key part of an overall governance and risk management strategy. The following are just a few examples of relevant controls in key regulations that align with IGA capabilities.

✓ **PCI DSS Section 7**
Implementation of an Access Control system that supports each user having a unique ID, providing only the rights they need for their specific job duties

✓ **GDPR Articles 5 and 6**
Proof of technical and organizational controls that define user access across systems, applications, and data, which can include:

- Access Management
- Access Governance
- Authorization
- Identity Management
- Identity Governance

✓ **SOX Sections 404 and 302**
Three controls related to Identity Governance:

- Centralization administration of access management and identity governance
- Enforcement of segregation of duties (SoD) policies
- Regular auditing to verify user rights and permissions across the infrastructure
- Automatic logging and tracking tools that generate clear reports for compliance audits

ServiceNow IRM Enriched with Clear Skye IGA: 7 Key Benefits

IGA is a key process within an overall risk management program. It is where many organizations start on their GRC journey. As programs mature, it is likely that most organizations will add a GRC software solution to oversee their risk management efforts.

ServiceNow's IRM solution is a recognized leader according in the Gartner GRC Magic Quadrant. IRM consists of four applications that can work together or standalone: Policy and Compliance Management, Risk Management, Audit Management, and Vendor Risk Management.

There are clear benefits to organizations that choose to leverage both IGA and GRC capabilities on the Now platform, such as seamless application integration, scalability, improved efficiency and productivity, and adaptability to an organization's specific business needs.

Being native to the Now platform, Clear Skye IGA offers IRM customers unique capabilities to enhance their regulatory compliance initiatives by feeding GRC with identity-related evidence.

IRM and Clear Skye IGA both being native to the Now platform can share information bi-directional to help manage risk. This provides three key sets of benefits: identity evidence, issue management, and compliance checks. For example, GRC Indicators have direct access to Clear Skye IGA and can pull evidence in real time.

Identity Evidence Collection via GRC Control Indicators

Clear Skye IGA has an Identity Warehouse built using the Now platform that contains all user accounts (of all types) and their associated security memberships. The more systems you select to integrate, the wider the net and more evidence can be fed into GRC. With this identity-rich data in ServiceNow, Clear Skye IGA provides these benefits.

Benefit 1: Near-Real-Time Identity Data

GRC risk indicators use evidence to determine whether a control is out of compliance. Clear Skye IGA provides evidence in real time.

Benefit 2: User Access Reviews/Attestation

Clear Skye performs all quarterly user reviews within ServiceNow. This means you also have access to all review decisions, review records, and campaigns.

Issue Management

Issues result from a compliance failure as identified by the indicators within the ServiceNow GRC framework. Issues are used to track the work caused by a control failure within GRC. Clear Skye IGA enriches GRC Issues Management in the following ways.

Benefit 3: Disable User Access Directly Within Issue

Compliance teams can remediate access directly within the GRC incident without the need to go to a standalone IGA system. Importantly, the access removal is added as supporting evidence to the Issue being resolved.

Benefit 4: Perform Ad Hoc Access Review Within Issue

An alternative to removing access is creating an ad hoc user access attestation. The attestation is assigned to the business manager or a specific group/user. This allows the business to directly engage within GRC issues and empowers the line of business reviewer to decide the correct path forward.

Benefit 5: Delay Action

In many cases the policy violation is not urgent, but it does need to be addressed in a documented fashion. Inline delayed actions enable your team to put their immediate focus on higher-priority issues while also ensuring that every issue is tracked and addressed by the right person at the right time.

Benefit 6: Acceptable Issue Generation

If an organization decides to accept a particular risk, you can create GRC issues on the fly instead of waiting for the issue to be detected in 90 days. These issues can be set up to require additional approval when necessary and/or to automatically cancel, based on specific risk criteria.

> “The ability to take advantage of **CMDB** and **Compliance (GRC-IRM)** information natively within the Identity Solution is **highly valuable** with Clear Skye on the Now Platform.”
>
> **TODD WIEDMAN**
> Chief Information Security Officer – Landis & Gyr

Proactive Compliance Check

Clear Skye enforces GRC controls during IGA workflow. Common examples include Identity lifecycle events such as onboarding and employee transfer, as well as access requests or access reviews. This enables organizations to take a proactive approach to compliance checks:

Benefit 7: Compliant Access Requests
Using the same indicators that usually check compliance requirements after something has happened, you now have the ability to view and verify compliance controls beforehand.

Conclusion

GRC comprises a wide range of processes and solutions that can significantly ease the pain of regulatory compliance as well as protect against costly breaches. Organizations typically embark on their IRM / GRC journey through IGA, though other starting points are not uncommon.

As organizations mature their GRC program, they need to consider how to efficiently link processes to more rapidly manage business risk. One way to ensure speed and effectiveness is to build as many of these processes on a single platform and data plane, ensuring that the program vision is never hampered by the technology choices made.

Clear Skye IGA and ServiceNow IRM, both running on the Now Platform, can provide a foundation to set up an organization for GRC success in both the long and short term. Clear Skye IGA supports organizational compliance through native integration with ServiceNow. Organizations benefit in a number of key ways, such as improved identity management and issue resolution. But the greatest benefit is the ability to take a more holistic and proactive approach to risk instead of just reacting to threats that have already taken hold.

About Clear Skye

Clear Skye is an Identity Access and Management (IAM) software company, reimagining enterprise identity access and risk management software to make a complicated problem easier to manage.

Built on ServiceNow’s Now Platform, Clear Skye IGA removes the need for a standalone IGA solution in favor of leveraging an existing platform.

Our Solution

Clear Skye IGA is built upon the ServiceNow Now Platform, which processes 4 billion transactions a month. Our IGA solution provides identity lifecycle management and governance solutions across a broad set of verticals.

The Clear Skye IGA software transforms security teams’ digital environments by finally aligning identity management with critical functions like ITSM, CMBD, GRC, and security operations into a centralized location.

Previously, companies relied on weak integrations to allow ServiceNow to perform IGA services.

Native to the Now Platform, Clear Skye removes the need for a standalone IGA solution in favor of leveraging an existing platform. All ServiceNow data, workflow information, and interfaces are readily available in the Clear Skye IGA tool.

To learn about a better way to IGA follow Clear Skye on LinkedIn, Twitter, and Facebook. Find those channels and more great content at clearskye.com >

LEARN MORE

Read Clear Skye customer testimonials and case studies at clearskye.com/resources >