Keylight

By NAVEX Global®

The Public Sector
with Keylight®

The Keylight Platform enables public sector agencies to gain better visibility into the policies they must follow, the risks they must manage, and the incidents they must address.

Imagine you work for a federal agency that was hacked, resulting in thousands of compromised Social Security numbers. Or perhaps you work for a city whose water supply is unsafe to drink for an extended period. Maybe your county government department missed a compliance deadline for a federal mandate, which the local press is now criticizing you for.

During the aftermath of a crisis, the emphasis is on minimizing the damage and restoring public trust. Once the dust settles, risk management thinking usually takes over. The question then becomes: Can we prevent this from happening again?

Effective risk management and compliance management require information that is complete, readily accessible, and usable, to enable quick decision-making instead of impeding it. Unfortunately, information in most organizations is maintained in disparate systems and/or spreadsheets, and managed by a variety of sources (e.g., departments). As a result, it often is outdated, hidden in nondescript network folders, and/or missing key data fields.

Minimize violations with efficient compliance and risk management
The optimal way to handle disruptive incidents is to:

- Comply with the regulations designed to prevent them
- Recognize and manage the risk of them occurring before they happen

Unfortunately, this is not always a realistic goal for government agencies that are saddled with outdated technology and fewer staff resources than in previous years. Further complicating these efforts are the abundance of compliance requirements and shifting regulations the typical agency faces.

As such, government agencies are usually reacting to crisis events instead of preventing them. The key to becoming more proactive is to put in place basic controls for the processes and regulations that help manage risk and account for every transaction. Agencies also need to confirm completeness through auditing activities. The objective is having an environment capable of:

- Generating assessments to gather sufficient information to adequately assess risks
- Housing standard policies and procedures
- Creating a risk register that lists and scores risks
- Linking risks to the organization's controls
- Creating awareness events

for validating understanding
- Sharing information (departmental and enterprise-wide) via dashboards and reports

Protect citizen data with better IT security management
Government agencies digitally store some of the most sensitive, personal information of their constituents, including birth records, Social Security numbers, tax information and medical records, to name a few. As such, they are a prime target of hackers.

The job of hackers is made easier by attempts to manage, identify, assess and analyze IT risks using out-of-date technology like spreadsheets and network folders.

Data breaches are some of the most disruptive crisis events a government agency can incur. Again, the optimal way to handle them is to prevent them from occurring, which requires more than just updated firewalls and anti-virus software.

Agencies need a complete view of their IT infrastructure, including a complete list of assets, a reportable risk register that scores IT risks, and a comprehensive view of threats and vulnerabilities to their networks. This requires a

tool that enables organizations to manage IT security efficiently and effectively by:

- Creating a centralized asset repository
- Tracking all risks and exceptions, from identification through the remediation process, associated with your IT risk management and security program
- Integrating findings from vulnerability, web application, and configuration scanners, SIEMs and syslog files for a holistic picture of your vulnerability landscape
- Assessing third and fourth parties for risk to the organization via dynamic assessments
- Linking risks to strategic objectives, Key Performance Indicators, Key Risk Indicators, and other benchmarks

Regain public trust with better crisis management
No matter how diligent one works to minimize risk and remain compliant, incidents may occur. A child may get injured at a city-operated park. One or more citizens may accuse a sheriff's deputy of inappropriate conduct. An elected official may use his or her office to embezzle funds or accept bribes.

Whether large or small, restoring the public's trust requires efficient crisis management, from discovery to investigation to resolution. This is accomplished by:

- Collecting a variety of incident reports, from information security events to anonymous whistleblowers and human resources reports, and prioritize them based on the calculated impact

- Performing initial triage on incidents by automatically routing incidents to their appropriate workflows based on type and/or severity
- Managing the incident lifecycle, from assigning response teams to investigation and remediation activities
- Preserving critical analysis such as incident discovery date, severity, evidence and prevention for future audits
- Storing incident data to enable officials to spot trends much easier than if information is contained in separate reports
- Creating continuity plans in case an incident causes disruption to the agency

Bring order to the chaos
You can bring order to this chaos with the Keylight Platform from Lockpath. The Keylight Platform consists of a fully integrated suite of applications designed to help manage all facets of compliance and risk programs.

Unlike most platform providers, Lockpath's goal is to implement the Keylight Platform within 30 days to yield a timely return on investment.

The platform provides ample flexibility and scalability to meet governance, risk management, and compliance ("GRC") needs at both an enterprise and departmental level. Some clients initially configure the platform for use in select areas of the organization (e.g., IT security, vendor management), with future plans to expand enterprise-wide, as they rollout an overall program. And rather than being a disruptive technology, the Keylight Platform can complement existing processes and resources.

Keylight enables users to:

- See the full impact of risks by linking them to policies, controls, assets, incidents and to business impact analyses

Keylight
By NAVEX Global

- Demonstrate transparency in audits with recorded data history and version comparison reports
- Consistently and efficiently manage incidents
- Encourage anonymous disclosure of internal incidents and violations
- Continuously monitor the effectiveness of risk and compliance programs through real-time reporting and dashboards
- Enforce process consistency with a robust workflow engine

The most efficient, intuitive enterprise-wide platform on the market

Compliance, risk management and security needs that exist today may broaden tomorrow, and concerns you don't have today will manifest when you least expect them. In the complex world of government, you can't settle for just any solution. You need one that:

- Scales so that it can be used by other departments or agencies
- Evolves alongside your risk, audit, and compliance programs in a code-free manner
- Adapts to your processes, rather than forcing you to adopt an unfamiliar paradigm.

The Keylight Platform was created by industry experts who recognized the need for easy-to-use software that was flexible and scalable to serve ever-changing and expanding organizational goals and objectives.

Unlike most providers of this type of platform, Lockpath's goal is to implement the Keylight Platform within 30 days.

Keylight is easily configurable, so it can adapt to changes in an organization's operational, regulatory, or security needs. In fact, while most platforms require additional programming and code-writing to reflect changes in a business environment, Keylight's point-and-click, drag-and-drop approach to configuring a solution removes programmers from the staffing equation, often resulting in faster results at a lower cost. This means that as risks and the regulatory environment change, the Keylight Platform is nimble enough to adapt and incorporate these changes.

If you're frustrated by the slow implementation of your current platform, still trying to retrofit your existing technology to meet new standards, or just throwing in the towel and hoping spreadsheets and other antiquated tools can do

the job, contact Lockpath at **info@Lockpath.com**.

About Lockpath

Lockpath is an enterprise software company that helps organizations understand and manage their risk. The company's line of integrated risk management solutions provides companies with the means to efficiently and effectively identify, manage, and monitor risks, for a more agile and resilient business. Lockpath serves a client base of global organizations ranging from small and midsize companies to Fortune 10 enterprises in more than 15 industries. The company is headquartered in Overland Park, Kansas.

18032206

Lockpath.
A NAVEX Global® Company