

IMPLEMENTING AN ENTERPRISE LEGAL GOVERNANCE, RISK, AND COMPLIANCE STRATEGY

LEGAL
GRC

exterro®

Implementing an Enterprise Legal Governance, Risk, and Compliance Strategy

The converging priorities among Legal, Privacy, Compliance, Security, and IT teams within global enterprises has created a new reality for **Chief Legal Officers** and **General Counsel** everywhere: Evolving regulations and laws mean that Legal departments now have greater influence over processes and technologies that can help mitigate increasing cybersecurity, privacy and compliance risks. Those risks can mostly be boiled down to how an organization manages their data.

Therefore, in addition to overseeing the legal operations of the organization, the CLO today must also play a central role in ensuring the company's compliance, privacy and data governance capabilities meet all regulatory obligations. The CLO must understand other enterprise risks facing the company, implement appropriate processes to prevent them from occurring, and quickly and efficiently address these risks should they occur.

Business challenges—such as complying with privacy laws or implementing robust data minimization policies and procedures—now span organizational units. Those challenges break down primarily into three major threats:

- › New data privacy laws that grant consumers new rights over their personal data
- › Data breaches and the resulting fines and reputational risk involved
- › Ensuring preservation of relevant data for criminal or civil litigation

Evolving regulations and laws mean that it is now simply not possible to take a siloed approach and expect to effectively address these business challenges. Single-point solutions can no longer solve these complex problems, either. Instead, a new strategy is required; a strategy that unifies different people, processes, and technologies that are utilized to ensure compliance, reduce risk and optimize operations.

Organizations now require a centralized technology framework that orchestrates all tasks, activities, and stakeholders involved in critical data privacy, data security, data retention, litigation and legal operations while seamlessly integrating into existing enterprise infrastructure. That central technology framework—a hub through which legal and compliance operations can be run effectively and defensibly—is the centerpiece of your **Legal Governance, Risk, and Compliance** (GRC) platform.

TABLE OF CONTENTS



SECTION 1

The Foundation of an Enterprise Legal GRC Platform p. 3

Where Does Your Data Live—and How Do You Connect to it?	Who Owns It?	Which Regulations Govern It?
p. 4	p. 4	p. 5

Which Third Parties Have Access to It?	Bringing Your Data Together with Technology
p. 5	p. 6



SECTION 2

Implementing a Legal GRC Strategy in Practice p. 7

New Personnel Roles & Considerations	The Importance of Process Orchestration Across Your Enterprise
p. 8	p. 9
	Data Subject Access Request (DSAR) Process p. 9
	Data Breach Notification Process p. 11
What Does a Legal GRC Platform Look Like in Practice?	The Future is Now
p. 12	p. 13



THE FOUNDATION OF AN ENTERPRISE LEGAL GRC PLATFORM

To comply with the three major, data-driven threats outlined above, the basis of a Legal GRC platform begins with knowing the corporate data governance strategy by which all sensitive and other business critical information is (or should be) handled. It's often a simpler question to answer than to showcase in practice.

To fully understand your organizational data, seek answers to the following questions, each of which is essential to hygienic information governance and regulatory compliance:

- › Where does your data live?
- › Who owns it?
- › Which regulations govern it?
- › Which third parties have access to it—and how do they use it?
- › How much data do you really have?

These are the basic, foundational questions that will make up a centerpiece of your enterprise Legal GRC strategy, with the data inventory acting as the engine that keeps the machine running. Keeping that engine maintained creates positive downstream effects that lessen risk throughout the business and help ensure compliance efforts are defensible.

Where Does Your Data Live—and How Do You Connect to it?

We know that data is what unifies different departments and business challenges. But how do you find all of the data that lives within an organization? Without a modern, enterprise-class data inventory, it's difficult to know whether that corporate data governance strategy is operating the right way.

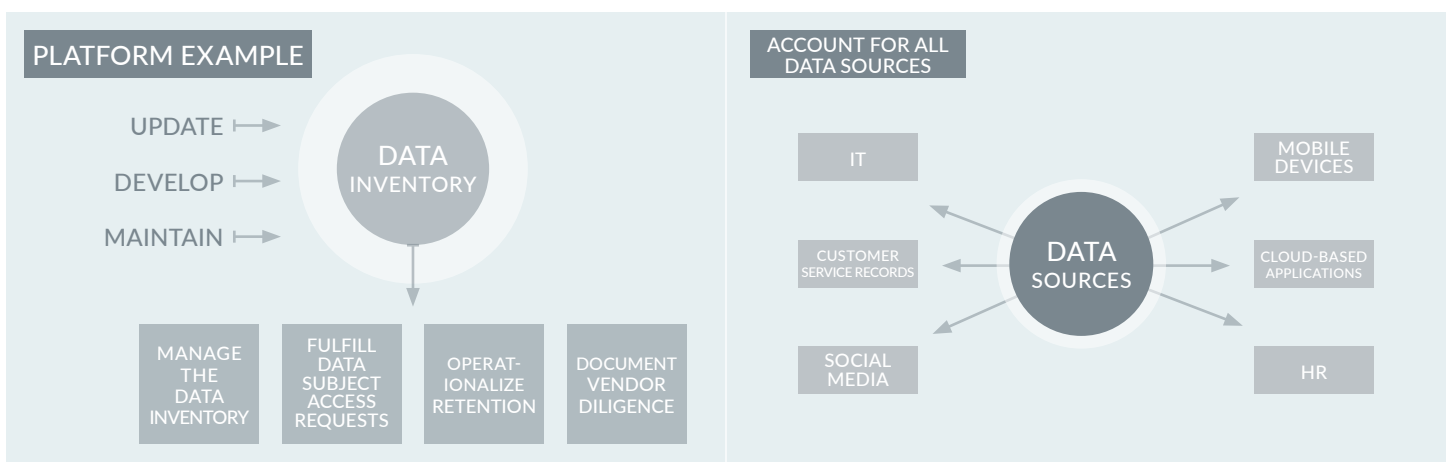
And what does a modern, enterprise-class data inventory look like? Put simply, it is a central location for identifying all of your organization's data—neatly identified and organized in a single platform—that must include a library of regulatory laws regarding retention, and guidelines for making informed decisions when choosing to remediate or otherwise take action with your data. Built in this way, data stewards are able to visualize all relevant data in one location, rather than having to seek out and hunt down disparate pieces of information from what could be hundreds of thousands of different shared drives, hard drives, or file cabinets across an organization.

To build a full, comprehensive inventory of your organizational data is no easy task; it requires time, effort, and investigation to get it right, and usually the help of a team experienced in understanding how to locate information across vast data plains. The team responsible for building the data inventory must have an understanding of the regulations that govern that information, because retention processes must also be taken into account: Is the organization holding data that could create legal hurdles in the future?

Choosing the right partner to help you build this inventory is critical: It often is the difference between projects lasting 30 days or six to 12 months or more. The right partner will help your company properly scope the project to ensure that organizational expectations for your data inventory are met. This usually includes access to customizable process templates that help leverage their expertise in the market, guidance on how to account for regulatory and corporate retention policies, in-depth assistance to ensure a quick and timely completion of the project, so that all stakeholders are happy.

Who Owns It?

Next to understanding where data lives, it's also important to understand who owns it: which departments, policies, and executives oversee its storage? Do the **stewards of this data** hold the appropriate certifications that help ensure they understand how to handle certain material? Cross-departmental communication with processes that run concurrently with one another can help different departments handle data properly, with direction from a unified executive team that understands the opportunities that an up-to-date data inventory can represent.



Which Regulations Govern It?

Nearly all negative legal impacts are created by data misuse or mismanagement. Most litigation and regulatory fines stem from one of the following data mismanagement issues:

- Retaining too much data (e.g. not following enterprise retention and deletion policies)
- Retaining too little data (e.g. spoliation, or lost data that there was a legal obligation to retain)
- Mismanaging custodian or consumer/user data (e.g. a data breach or incorrect DSAR fulfillment)

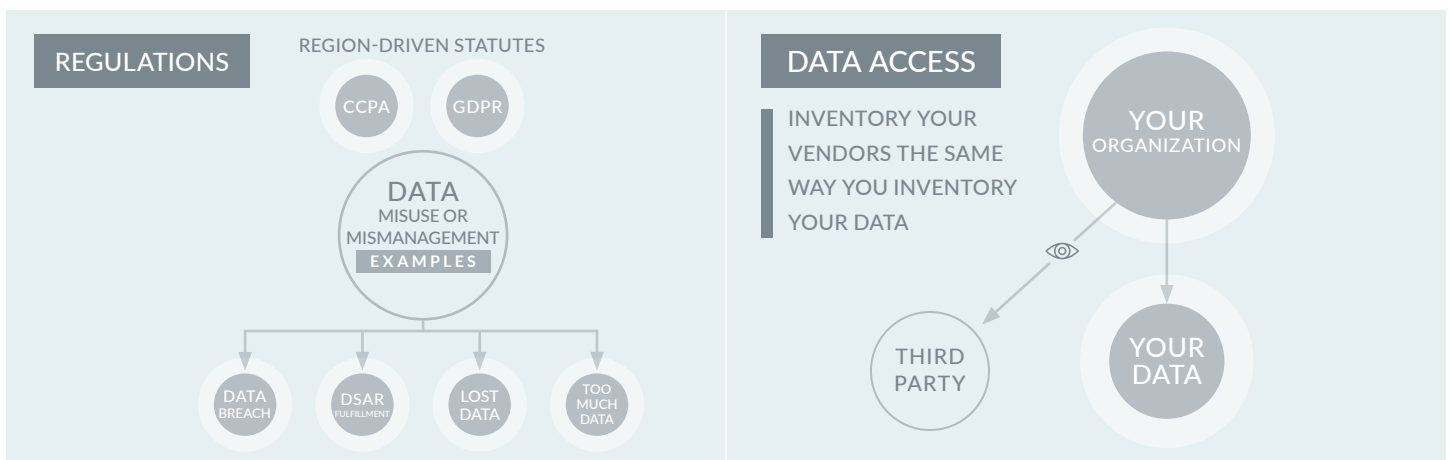
Knowing the regulations helps you understand why certain data is stored in the first place. If the organization isn't holding the data for a business purpose, then it should be for a regulatory or other legal purpose, like a legal hold. There are scant other defensible reasons for keeping excess data, because excess data represents risk.

Breaches are an example that represent just one potential legal pitfall. Ensuring the laws that govern personal data are followed for specific, region-driven statutes like the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) requires a more sophisticated, knowledge-rich process. This is because these new privacy laws are more precise regarding obligations to delete personal data if it has served its business and legal purposes. **Reviewing retention guidelines should therefore be a regular part of data inventory maintenance.**

Which Third Parties Have Access to It?

In many cases, third parties represent an additional layer of risk, flying under the radar with the focus on data housed by your enterprise. But by some estimates, third parties represent the biggest risk when it comes to data breaches. This goes beyond high profile cases like General Electric's recent breach via a Canon subsidiary—rather, most companies that have suffered a breach saw it occur via lax third-party cybersecurity, according to the Ponemon Institute.

Due to the potential for a breach disaster that leaks critical business or consumer information, it's crucial for your organization to inventory your vendors, much in the same way you inventory your data. Understanding what information third parties have access to, how they're using it, and how they're securing their systems is critical information to having an accurate barometer of the risk they represent.



Bringing Your Data Together with Technology

Access to information about your data across your organization is the most critical, foundational element for an effective Legal GRC program. But on its own, it's not enough: Connecting to and validating that data is the next most important step. Validating the data is crucial to following every law pertaining to electronically stored information—spanning data privacy regulation compliance, retention requirements, and litigation requirements—and is critical to most business functions. Therefore, when considering a platform upon which to build an enterprise-class data inventory, the **CLO/GC must consider** technology that operates within a single, centralized framework solution, and is able to:

- A. Connect to each data source within the organization and validate the information;**
- B. Find hidden, rogue data**
- C. Integrate with other legal technology that is utilized across the enterprise;**

Only by connecting to each data source within an organization—including through integrations with existing technology—can you validate that your data inventory is up-to-date. Furthermore, you gain the ability to answer the next question after “what data do I have?”—which is “And how much data is there?”

This often includes uncovering rogue, or “dark” data, which by some estimates comprises as much as **80%** of the data at most organizations. This is data that might never have been found without the ability to connect to those sources. Because many legal and regulatory fines have to do with the ability to act on the data that an organization stores, being able to identify all data related to a specific request is especially important to legal compliance.

And because there is no single platform or end-to-end technology that can perform every task related to Legal Governance, Risk, and Compliance on its own, the final takeaway for CLOs is that the ability to connect to and integrate with other applications is key. Having a central platform with enterprise-class connectors means having the ability to integrate that technology into the new workflow processes you'll be building. These integrations ensure that all data is uncovered and can be correctly identified when needed during certain processes, which we'll explore in **SECTION 2**.

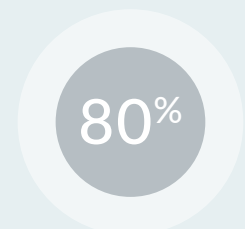
To comply with major regulatory hurdles facing global corporations today, both a data inventory and enterprise-class connectors are the critical components to being able to take action and remediate data when needed. In the next section, we'll take a closer look at how you can use your data inventory and connectors to orchestrate workflows that allow for efficient compliance.

NOTE:



MUST CONSIDER TECHNOLOGY
THAT OPERATES WITHIN A SINGLE,
CENTRALIZED FRAMEWORK SOLUTION

IT'S ESTIMATED THAT
MOST ORGANIZATIONS
HAVE AS MUCH AS →



OF ROGUE, OR
“DARK” DATA



IMPLEMENTING A LEGAL GRC STRATEGY IN PRACTICE

Enterprise-wide changes to your legal, compliance, privacy and information governance strategy are necessary to comply with new and coming data privacy and other regulations. These business challenges expand beyond the traditional siloed departmental approaches and require cooperation and consistent enforcement of policies across the enterprise to ensure total compliance. But on a practical level, breaking down these silos means enforcing cross-communication and working inter-departmentally to be aligned on process and achieve the same goals.

It does little good to build new processes to ensure the success of a new data management technology if people aren't able to perform those processes and properly utilize that technology. The success of any risk mitigation program is dependent on how stakeholders in the organization embrace the realities of their changing priorities and implement these new processes in their departments—including training to improve competencies surrounding new technologies and processes. Below, we'll take a more thorough look at the three key tenets of any successful business strategy: *people*, *processes*, and *technology*.

New Personnel Roles & Considerations

Implementing changes in personnel could come from a number of different needs: Some businesses may find that their current organizational chart isn't set up to successfully manage the **Legal GRC challenges** they're facing (or will face in the future), while others may find that they are lacking personnel with the key skills required to manage and reinforce these changes. Regardless, given the transformation that some departments will likely need to undergo over the coming years, there are three main phases for change management consideration:

- › Preparing your people for change
- › Managing the change process
- › Reinforcing those changes with your workers


To understand the scope of the changes necessary in your department, it's helpful to have a strong grasp on both current business processes and the forecasted processes that are necessary to the success of your business—like efficiently responding to a consumer request, or defensibly following up on a security incident. Start by determining answers the following:

- › Which team leaders and employees are involved in current processes, and how/whether those individuals will see their workload and job duties change
- › How these changes will affect current process bottlenecks—and whether these departmental changes will expand or shrink those bottlenecks
- › What technologies are currently used by different departments and stakeholders to accomplish tasks, and whether they have the capability to help other departments perform their functions
- › Secondary to that, are there technology gaps that need to be filled to ensure that these changes happen effectively?


At this stage, start with your top-level people: Assess the culture and resources of your teams, convey the importance of messaging these changes and why they're occurring, and create ownership with your team leaders. Everyone should agree on the desired end-state, and what these changes will allow departments to do to successfully manage and implement the Legal GRC strategy. Once your senior leadership has a firm understanding of the destination, they'll be critical in making the journey a success; ultimately, your team leaders must be the zealots working to create these changes at the employee level, and their influence is invaluable. They will be critical in reinforcing these processes at every layer within the department, helping to create a cascading effect that touches everyone affected by these changes.

Determining how best to alter your Legal department is not likely to be fast or easy, but transformation that occurs over a long period of time is not a negative: There is ample time for reassessment and project check-ins to ensure that goals are met gradually through the weeks and months that encompass re-organization.


NEW PERSONNEL ROLES & CONSIDERATIONS



PREPARING
YOUR PEOPLE
FOR CHANGE




MANAGING
THE CHANGE
PROCESS



REINFORCING
THOSE CHANGES
WITH YOUR
WORKERS

START WITH THE TOP

ONCE YOUR SENIOR LEADERSHIP HAS A FIRM UNDERSTANDING OF THE DESTINATION, THEY'LL BE CRITICAL IN MAKING THE JOURNEY A SUCCESS



DETERMINING HOW BEST TO ALTER YOUR LEGAL DEPARTMENT IS NOT LIKELY TO BE FAST OR EASY

The Importance of Process Orchestration Across Your Enterprise

A key component of Legal GRC is building process synchronicity across all levels of the business, which ensures that all departments are communicating with one another internally at the correct times—this is critical to ensuring that Legal, Privacy, Compliance, Security, and IT teams are all on the same page. Process orchestration is made possible by automated workflows that are designed to fulfill specific requests; depending on the complexity of the request, each workflow could be routed dozens of directions before ultimate fulfillment.

Although there are a number of processes a business might choose to orchestrate, two in particular both illustrate the need to implement a Legal GRC strategy and are crucial to successful compliance with new data privacy regulations: the “right to know” (DSAR) process, and routing the data breach notification process.

Orchestrating the Data Subject Access Request (DSAR) Process

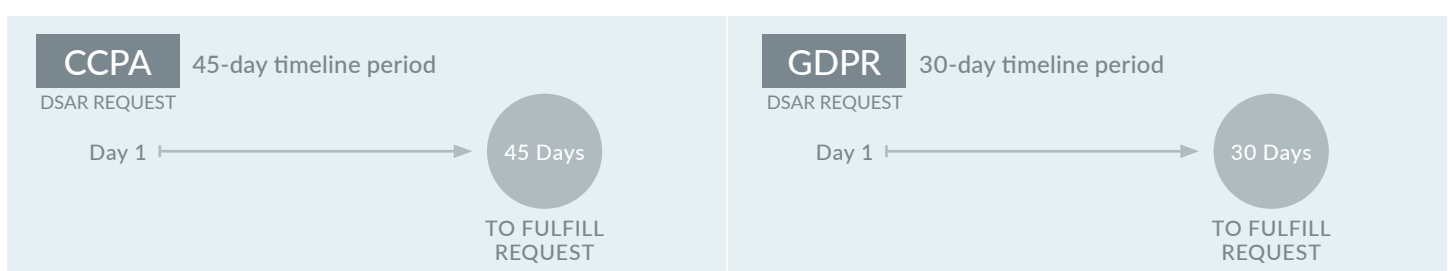
When an individual exercises their “right to know” what personal data an organization holds on them, the CCPA and GDPR mandate a fulfillment of that request within 45 days and 30 days, respectively. Along with each of these, there are a number of other notification requirements to fulfill, such as confirmation of receipt of the request. Numerous accounts—from analyst firm Gartner’s reporting on DSAR fulfillment to survey data on enterprise difficulties with compliance—have showcased that the DSAR process is more time-consuming, expensive, and complex than most businesses expected, as fewer than half of all organizations say they can meet the GDPR’s request deadlines.

Under the GDPR or CCPA, an individual might request any of the following:

- › The categories of personal data your organization holds on them
- › A copy of their personal data
- › Deletion of their personal data
- › Opting out of the sale of their personal data

At its heart, the technology your organization chooses to help fulfill DSAR requests must be able to do four things:

- 1. Request intake**
A structured web form, which includes residency, relationship to the company, name, email, address, and request type, is the simplest method for DSAR compliance.
- 2. Identity validation**
One of the first challenges an organization faces is in rooting out fraudulent requests. Connecting to a consumer loyalty program, or integrating with online identity validation services, can allow for challenge questions that help prove defensible processes on your end.
- 3. Information processing**
Routing the request through the proper departments to collect the correct information. This may involve including records managers and legal operations team members that can help with collection and reviewing the data and any necessary redactions and deletion of sensitive material. If deletion is requested, it’s critically important to evaluate whether the information is under a legal hold or another regulatory retention obligation.
- 4. Secure fulfillment**
The information must be sent to the requestor via secure means.



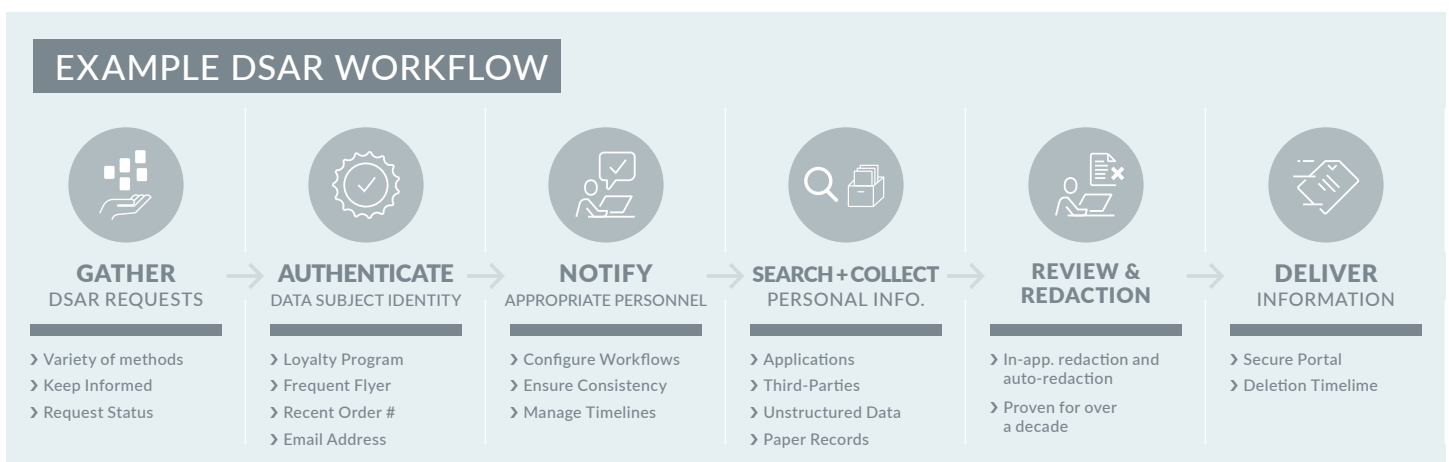
Orchestrating the Data Subject Access Request (DSAR) Process - continued

Due to the cross-functional nature of these requests, your DSAR technology should offer the ability to bring all teams and functions together in a streamlined way to adequately address the primary compliance concerns of every division stakeholder. A library of up-to-date regulations regarding data retention is invaluable at this juncture because it allows you to confirm whether you can actually remediate the data in a way that is consistent with what the subject requests (usually the deletion of data), or if you must alert them of a regulatory obligation that prevents you from completing that request.

As we discussed in section one, your Legal GRC platform must be able to connect to and find all data across an entire organization, and fulfillment of these requests is a key reason. Depending on the size of the organization, this could be no small feat; the request could stretch across several physical locations with disparate teams that must work together to ensure compliance. This also includes paper records—physical copies count as data, and they often come up in lawsuits because paper can be difficult to produce. That’s why automated workflows that include searches for physical records are such a critical element of the process of fulfilling a DSAR: it helps ensure that no rock goes unturned, and no risky data is left behind.

With an automated workflow, each step is customized based on the type of request (is it a consumer request, or a request from an employee?), the type of remediation that the individual is seeking, which team or individual the step is assigned to, and the duration in days that they have to fulfill their step in the workflow. All other platform technologies—your organization’s data inventory and regulatory or corporate retention schedules, for example—will then help inform and fulfill each step in the workflow as each team within the organization completes their respective task(s).

These workflows can run in parallel with other processes or in a traditional linear style. Given the short timeframes for request fulfillment, and the struggles that businesses have had in completing these requests on time, building custom workflows that automatically kick off the next step once the last one is completed can create major efficiencies in DSAR fulfillment, and help ensure a timely return of the data request to the subject.



Orchestrating the Data Breach Notification Process

When it comes to data breaches, the best-case scenario is that they don't happen. Even with high-end cybersecurity and strong vendor management/profiling to protect against increasingly-common third-party breaches, data breaches can still happen.

All 50 states now have data breach notification laws in place, and a number of industries also have their own sets of incident documentation laws. Incident reports may be used in litigation as a way to help prove a defensible process was in place when the incident occurred—they show that reasonable, repeatable processes were in place and properly followed, including appropriate reporting to the authorities (if necessary) and notifying individuals affected. Some of these laws don't necessarily require notification of a regulatory authority, but do require a consistent, documented follow up.

Whether it's a breach or another incident that has occurred, communication is key. A number of remediation steps must take place, starting with identifying the scope of the breach or incident—how far-reaching is it? Based on the scope of the incident, reporting it to regulatory authorities may be necessary. A consistent and defensible process can help mitigate business liability by showing that a reasonable procedure was followed. Proving that all standards were met is going to provide defensibility during litigation, because it offers true transparency and an audit trail to see how each step was completed.

It's important to note that while the **GC/CLO** is not responsible for physically protecting data or other company assets, they are the best person to quarterback these situations given that a number of steps must be performed in concert with laws surrounding the notification/response process. A basic **outline of a breach response** might look something like this, but with depth that may stretch into several potentially-conflicting statutes:

- › Validation of the data breach
- › Identifying remediation requirements, including compliance with breach notification regulations
- › An investigation into the breach, with documentation
- › Internal communication and coordination with appropriate authorities, as needed
- › Notifying the data subjects of the breach

Much in the same way that the **DSAR process** is best orchestrated with automated workflows, the breach notification process can be established in a way that touches all key stakeholders—Legal, Compliance, Security, IT, Records Management—to ensure that the right response notification process is implemented. This includes structuring the workflow during the breach validation and the breach investigation processes, and automatically documenting the processes with an audit trail to offer the regulatory authorities that govern the breach.

Under the GDPR, Data Privacy Officers have **72 hours** to alert the Supervisory Authority of a breach, which includes a description of the nature of the breach, the categories of personal data affected, and the approximate number of subjects affected. That's a lot to find in just three days, and automated workflows running parallel can help ensure a tight response process.

NOTE:

THE

GC/
CLO

IS NOT RESPONSIBLE FOR
PHYSICALLY PROTECTING DATA
OR OTHER COMPANY ASSETS

BUT



they are the best person to
quarterback these situations
given that a number of steps
must be performed

What Does a Legal GRC Platform Look Like in Practice?

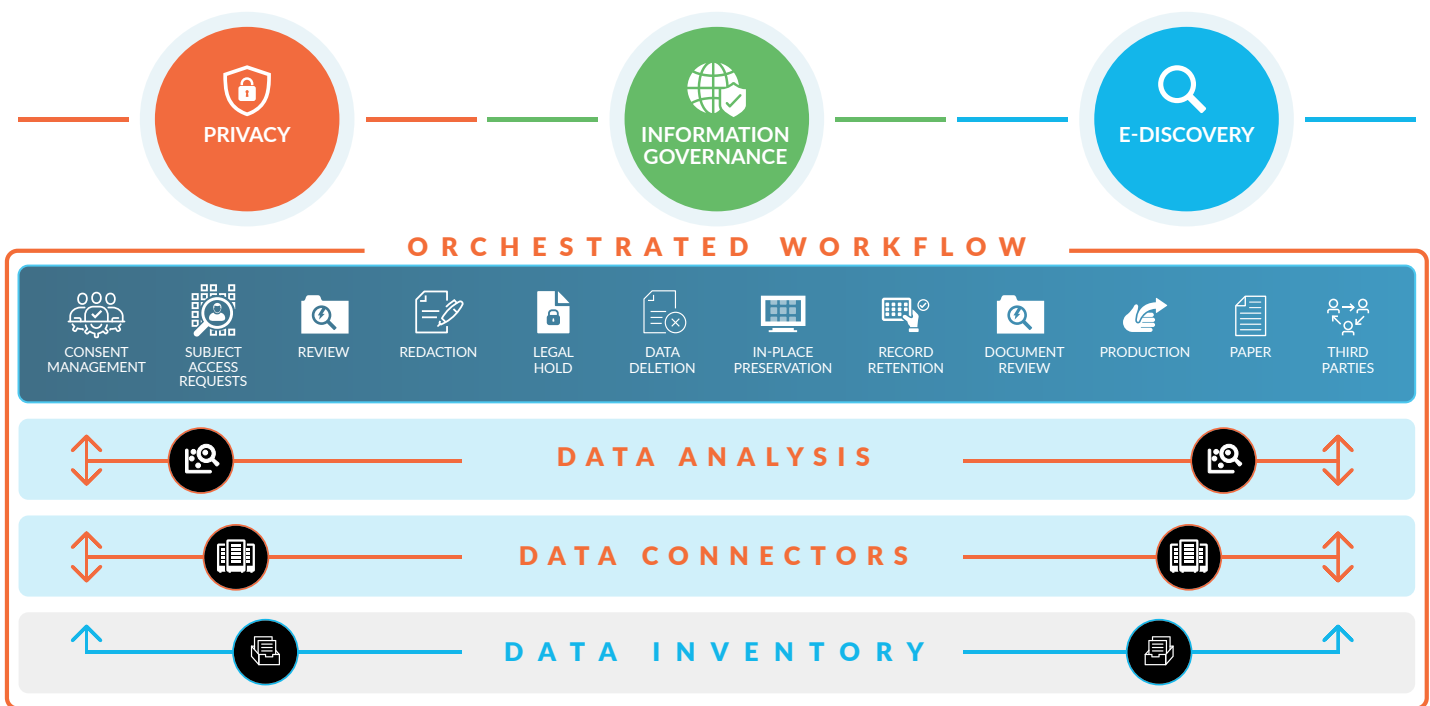
While there is no one, single platform that can cover every legal risk, it is possible to build a universal command center from which all of these processes can be managed. Because all of these GRC concerns stem from data, transparency and insight into organizational data is the key need from which your strategy must operate. Evolving regulations and laws mean that it is simply not possible to continue to view data from the individual business silos within an enterprise. Largely, that is why this new strategy is required: It unifies the different people, processes, and technologies utilized to ensure compliance, reduce risk, and optimize operations.

What is needed in addition to this new strategy is a centralized technology framework that orchestrates all of these activities across departments, meets the requirements of stakeholders involved with the critical functions of data privacy, data security, data retention, litigation, and legal operations, and integrates into your existing organizational IT infrastructure.

So what critical capabilities should your organization’s Legal GRC platform have? What are the hallmarks of a platform and strategy that can effectively navigate today’s challenges, as well as the legal and regulatory challenges ahead? We see four critical components:

- › **A comprehensive data inventory.** As we’ve explored, this is the foundational element to meeting most regulatory and legal obligations. The data inventory provides insight into where the data is, how much you have across your organization, and the laws that govern the use and storage of that data.
- › **An integrated platform.** A central solution that shares data and has the capability to integrate with other technology and tools in use across the organization.
- › **Process orchestration.** Automating as many workflows as possible helps ensure tasks are properly assigned and delivered to the correct teams at the right times. This also helps proactively address potential issues before they result in costly delays.
- › **Easy accessibility.** Your platform should be accessible by the correct stakeholders from anywhere, anytime, with security and privacy controls.

Generally, most business risks, compliance and regulatory issues likely fall under the Legal GRC umbrella, and the more interconnected and developed your organization’s risk management becomes, the better suited you are to help future-proof the enterprise.





The Future is Now

Priorities among Legal, Privacy, Compliance, Security and IT teams are now increasingly running parallel to one another. These changes are driven not by the competitive landscape, but by legal changes that are expanding the rights of people around the world. With the right strategy in place—one based around the core tenets of Legal GRC—these rapidly accelerating risks can be successfully managed and mitigated at enterprise organizations around the globe.

exterro[®]

See first-hand what Exterro's e-discovery and privacy technology can do for you.

www.exterro.com