Governance, Risk, Compliance, and APIs

Introduction

Application program interfaces (APIs) break new ground with respect to governance, risk, and compliance (GRC). By their nature, APIs are meant to enable transactional business activity without prior restraint, and they are major tools for innovation and experimentation. APIs save organizations money through reuse and consistency. These characteristics can ultimately make governance easier.

At the same time, APIs provide access to business assets that are sensitive, valuable, and must be protected, which raises GRC concerns. This paper shows how GRC and APIs interact in today's enterprises. Furthermore, it shows that using an API management platform can streamline governance and compliance.

An API by Any Other Name

The term API comes from programming. Although APIs have many applications, particularly in a business-to-business context, APIs are also what are driving the explosion in apps on mobile devices of all types.

If you're unfamiliar with APIs, we recommend watching the Containerization video from the authors of *Trillions*, which likens the impact of standardizing APIs to the standardization of shipping containers.

The Role of APIs in Contemporary Businesses

APIs are a fact of life in contemporary businesses and their role will only grow. Some firms now channel more than 80% of all digital traffic through APIs. APIs can be used to:

Manage the disruptive forces of mobile and distributed channels. It's vital for businesses to present a consistent experience to the customer, regardless of how the customer accesses the business—in person, online via desktop or mobile, or via phone. APIs help standardize the experience across channels while protecting core IT assets.

Provide a trusted means of information exchange. There are plenty of ways to interact with a company's information online, but activities such as screen-scraping disadvantage both the consumer and the producer of the information. With an API, the information owner knows who's asking, and the consumer knows that the information comes straight from the source. APIs provide a sort of façade for the enterprise, insulating data requesters from vendor changes, patches, and upgrades as well as IT operations in the background, giving everyone a consistent interface and a central point of contact and control.

Support application development. Instead of writing a custom integration from a company's core systems to a line of business or external application, APIs provide a standard interface that provides the right combination of data security and ease of access to facilitate useful applications with fast time-to-market.

Unify backend systems. Many companies use APIs for purely internal reasons. They may have hundreds of systems in place, with different systems in different divisions, not to mention the number of systems from mergers and acquisitions. Using an API internally can hide all that complexity and provide a central point of control that improves governance by offering visibility from one point into all the interactions with myriad backend systems.

Support market expansion. Through security keys and support for common protocols such as PCI, APIs provide a secure and efficient way to expand the market share of a company, so authorized third parties and new lines of business can easily interact with core systems without requiring changes to those systems.

Despite their business benefits, APIs may still concern some risk officers, as they open up new possibilities that standard GRC models may not have considered. In the next section, we consider the implications of several GRC frameworks for APIs, to provide business context.

Governance

The importance of enterprise risk management (ERM) has grown exponentially in the past few years, with the news filled with allegations of predatory lending, falsification, embezzlement, rogue trades, data leaks, and runaway algorithms. In response, the academic and business communities have accelerated development of governance frameworks. It's useful to review how frameworks apply to APIs since APIs are a substantial communication vector for many companies.

One such framework is CLASS,[1] which identifies five key elements of corporate governance.

[1] *Stephen A. Drew, Patricia C. Kelley, and Terry Kendrick.* "CLASS: Five elements of corporate governance to manage strategic risk," *Business Horizons,* 2006, vol. 49, issue 2, pages 127-138.

Culture. The authors of CLASS cite culture as a critical failure point for enterprises, particularly if failure is not an option. The result is excessive risk-taking, rule-bending, and gaming. An ethical and effective corporate culture encourages innovation, integrity, and openness balanced with reasonable levels of risk.

- The security provided by a centrally managed API platform supports a positive culture by fostering a safe proving ground for innovation while providing an effective way to enforce rules.

  In a culture of innovation, tempered with control, the central values of governance are reinforced. For example, a retailer, content, or consumer product company might want to reinforce the culture that protects the brand. Having an API program and platform that limits brand risk by eliminating inconsistent interaction experiences helps achieve the C in class.

Leadership. Good leaders show sensitivity to the needs of internal and external stakeholders. A big aspect of leadership in the coming years will involve granting or denying access to the company's electronic resources. The pressure will be on to do this rapidly to meet demanding business objectives. Failure to accommodate requests in a timely manner will result in delayed business initiatives and raise the possibility of rogue behaviors by frustrated requesters.

- A well-managed API platform enables disparate lines of business, customer, and partner constituencies to launch new initiatives, but provides a level of control so that strong personalities don't build one-off applications that circumvent corporate objectives or security standards.

  Additionally, when enterprises have an established API program and processes, they proactively lead the market, partners, and employees by creating a framework for using data properly. The API management platform enforces proper data usage by offering data in a particular, governed way, making the job of governance easier.

Alignment. More than ever, enterprises must align key functions and responsibilities in the face of rapidly changing business environments. Aligning systems to support an appropriate level of risk-taking and striking a balance between entrepreneurship and conservatism involves developing a common language and resolving conflicts between functions. Information systems must support enterprise risk management. Additionally, the activities of executives, risk management, and rank-and-file employees must align to ensure compliance with regulations such as **Sarbanes-Oxley** (SOX), **PCI**, and the **Health Insurance Portability and Accountability Act** (HIPAA), to name a few.

- API management platforms support government and industry standards for information exchange (conservatism) as well as rapid development and iteration (entrepreneurship). Alignment can be achieved through the assurance that data propagated from core systems is consistent and controlled.

  By definition, API management platforms provide a rich, robust set of technologies and tools that allow the implementation of good governance processes. API management platforms are tools for creating and enforcing policies of all types. Yet they allow innovation and execution of aggressive business objectives.

Systems. In the wake of the financial scandals of the early 2000s, SOX was enacted (along with numerous other regulations). Under SOX, executives must attest that the data submitted was accurate and since this attestation carried the possibility of personal liability, compliance is serious business. COBIT (Control Objectives for Information and Related Technology) is the most common way that companies in the US comply with SOX (see the COBIT sidebar).

- An API management platform is designed to mediate between multiple systems and parties inside and outside the enterprise, through a consistent set of standards, offering the maximum in flexibility and role-based control.

  After a transaction has occurred, API management platforms can create output logs and reports in the desired format appropriate for a given regulatory audit, showing who accessed what data and whether, if necessary, it was properly masked to obscure personal information.

Structure. Companies must be structured to support risk controls. Best practices in enterprise risk management recommend decentralizing risk evaluation, placing responsibility in the hands of those most directly involved in each process of daily operation. An effective system of checks and balances is also critical.

- An API management platform uses standardization and a consistent interface to support safe experimentation and iteration by small groups with localized or specialized expertise, as well as role- and group-specific risk controls.

  API platforms and strategies also allow a choice of approaches and layers of governance at different stages of an application lifecycle, or at different stages of an emerging business or partner lifecycle.

COBIT

Although COBIT grew in the wake of the passage of SOX, it is a robust and comprehensive framework for ensuring accountable systems. As a result of this, businesses around the world have adopted COBIT. Because it's so comprehensive that it tends to be overkill (governance and compliance needs vary per company), organizations tend to implement a subset of COBIT or to say that their governance process maps to particular portions of COBIT.

More important than the details of COBIT itself is the fact that the best API management platforms can provide the flexibility to implement your governance process, no matter how much or how little of COBIT it maps to.

Compliance

Management consulting firm Baker & McKenzie has outlined elements of corporate compliance,[2] which are instructive in setting up a framework for understanding and resolving the compliance issues raised by APIs, which API management platforms can help resolve.

Risk assessment. Companies must constantly scrutinize new business partners and third-party agents. In the world of APIs, there will be more of both.

- API management platforms allow for the creation of individual or tiered sets of controls, both before a partner signs on and during ongoing operations.

  For example, if a partner or app intentionally or accidentally misbehaves, they can be selectively disconnected while the rest of the customers and partners continue to be connected and protected.

[2] "5 Essential Elements of Corporate Compliance: A Global Template," Baker & McKenzie, 2012.

Standards and controls. Companies must establish stringent protocols for screening business partners and third parties, including contracts with provisions that give the company the right to monitor partner conduct.

- API management platforms can be used to enforce service level agreements, conduct traffic control, and encrypt data securely. When a single platform is used as an intermediary between core systems, lines of business, and the outside world, inaccurate records are caught much faster.
- API management platforms also provide a way to control who receives corporate data and information assets.

  They can be used to protect corporate assets such as brand information or to ensure that licensing agreements with third parties are followed, as well as to comply with any international laws that stipulate where data may and may not be distributed. In this way, API management platforms automate compliance.

Training. Enforcement trends and government regulations change quickly, particularly for companies with a global presence.

- The API GRC team described under Leadership should set training policy and constituencies based on changing API functionality, strategy, and reach. Above all, an API platform is meant to allow quick responses to changing business regulations and conditions.

Oversight. Companies should establish a regular monitoring system to spot problems and address them. It's especially important that such a system can quickly identify and remediate problems and compliance issues.

- API management platforms can provide a complete audit trail of all data consumption from and contribution to enterprise systems, an important aspect of compliance.

An API management platform is a tremendous asset for governance and compliance because it creates one central place for risk officers to gain visibility of data flows and enforce governance policies. Without an API management platform, organizations run the risk of supporting multiple electronic entry points and single-purpose integrations with partners, which may be happening completely unsupervised and out of view of GRC officers.

Without centralized control, risk officers must attempt to consolidate visibility and reporting on the identity of access requesters and the nature of their data transfers across multiple, inconsistent interfaces. Additionally, advanced API management platforms can enforce layers of rules that apply separately to each level of the organization's hierarchy; the 401(k) division might not have the same rules as the dental insurance division of a financial institution, for example.

Case Studies

An API management platform can address most GRC issues introduced by APIs.

Legacy Layering at a Major Retailer

One major US retailer that is especially sensitive to brand issues uses an API management platform to manage its governance, risk, and compliance issues.

Challenge: The retailer faced an issue familiar to many businesses: How to maintain a consistent interaction experience with the company—no matter where and when the interaction occurs—and enable innovation, while protecting core assets?

The reality is that both employees and customers want to see the same product information, the same prices, and a consistent look and feel no matter how they access the company's systems. But many of the core legacy systems of the company were not flexible enough to keep up with the pace of change dictated by such business requirements.

Solution: Using an API management platform as the backbone of its strategy, the retailer devised a three-tiered scheme. On the bottom are core business assets, systems, and data (such as master customer records in a CRM system), which change infrequently. In the middle are differentiating capabilities that change somewhat more frequently and execute the transformations that bring transactions to life. On the top layer is the user interface, which could be a channel offer to an online customer or a check stand employee screen, which might change every few days or even hours. The API capability exposes the necessary business rules and data to help create a consistent experience while allowing a faster pace of innovation than core systems can support.

Each layer also reflects a number of users. The top layer supports the greatest variety of users (such as an individual receiving a customized offer); the middle supports the functionality of a given group or consumption framework (such as the call center, roving floor personnel, or mobile app developers); and the bottom layer handles master data management (MDM) and core processing. By necessity, this layer changes the least and is available to the smallest number of people.

Providing consistent and standardized access to data via APIs allows auditing, governance, and risk controls to be put in place in the API management platform. Controlled access via APIs also helps assure that data can be trusted.

For example, a developer who builds a channel sales app that connects to a retailer knows that prices, product information, and store locations are accurate; likewise, the retailer knows that the developer is a trusted party because of the API key that uniquely identifies that developer. By insulating the core data and business rules, it both creates reusability and consistency in the experience and also enables easier adherence to compliance, governance, and security requirements.

With the exchange of API keys, as well as authorization and authentication, innovation and expansion can happen securely and faster. And, once the link is established, the centralized API management system makes traffic auditing easier, reducing the scope and cost of compliance efforts overall.

Data Governance at a Financial Institution

A large financial institution with insurance and brokerage arms has many regulations to consider, including SOX, HIPAA, and various Securities and Exchange Commission (SEC) regulations, as well as many insurance laws.

Challenge: The company was concerned with attestations about data access. Executives were obligated to sign affidavits stating that no prohibited parties gained access to protected data. The venerable company had grown by acquisition over 150 years, and as such, many internal silos existed, preventing straightforward data sharing.

Solution: The company implemented an API management platform that governed all interdepartmental and external interfaces. For the first time, the company had true visibility into which parties were accessing which data. Importantly, it also had a central "choke point" of enforcement, affording the ability to instantly cut off access to malefactors or stop violations before any damage could be done.

The fine-grained reporting platform increased the depth and strength of the verification processes that supported the company's regulatory compliance documents. Regulations constantly change; it is much easier to implement a change quickly across a centralized platform than through multiple nonstandard interfaces.

Benefits for Governance and Compliance

API management platforms can help organizations manage the complex and ever changing issues surrounding governance and compliance. They provide access controls to ensure auditability and provide confidence for attestation when executives must sign on the dotted line.

At most large companies, a larger percentage of traffic coming to the data center is API traffic. The more API traffic you have, the more an API management platform can streamline and centralize governance.

Further, API management platforms:

- Offer a valid control point to apply enterprise governance policies
- Provide visibility into all access to backend systems that comes through the API, which may be enough for compliance purposes in some cases
- Enable flexibility to grant access to resources or to remove that access
- Offer a single point to implement governance in the face of changing regulations, streamlining the ability to respond to changes at least for traffic that comes through APIs
- Offer hierarchical control that mirrors your organizational structure. If you need separate rules for one division, rules can be applied to only that division.
- Allow you to decommission older systems behind the scenes, saving money without impacting those using the API

Conclusion

APIs save businesses money and provide new levels of business agility through reusability and consistency. These very characteristics ultimately make the task of governance easier. An API management platform provides a central point for interactions with the enterprise's core systems, providing a new level of visibility, control, and auditability. This should come as welcome news to those in charge of governance and compliance who have been concerned with the proliferation of partners, apps, and devices so common in today's enterprise.

For further inquiry

If you'd like more information on Apigee's API management for SDN, please email info@apigee.com or send a message via Twitter to @apigee.

About Apigee

Apigee is the leading provider of API technology and services for enterprises and developers. Hundreds of companies including AT&T, Bechtel, eBay, Korea Telecom, Telefonica and Walgreens, as well as tens of thousands of developers use Apigee to simplify the delivery, management and analysis of APIs and apps. Apigee's global headquarters are in Palo Alto, California, and it also has offices in Bangalore, India; London; and Austin, Texas. To learn more, go to apigee.com.

Find Best Practices to Accelerate your API Strategy

Scale, Control and Secure your Enterprise

Build Cutting-Edge Apps and Intuitive APIs

Apigee Corporation
260 Sheridan Avenue, Suite 320
Palo Alto, CA 94306, USA
Tel: +1 (408) 343-7300
sales@apigee.com