Brought to you by:

Red Hat

Open APIs in Financial Services

for dummies®

A Wiley Brand

Understand what APIs can do for you

Design open API strategy for changing needs

Create and manage open APIs

Alessandro Petroni

Alfonso Navío Francés

Eric Marts

Red Hat Special Edition

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications; develop cloud-native applications; standardize on its industry-leading operating system; and automate, secure, and manage complex environments, and mission critical applications. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future. Learn more at redhat.com/financial.

Open APIs in Financial Services

Red Hat Special Edition

by Alessandro Petroni, Alfonso Navío Francés, and Eric Marts

for dummies®
A Wiley Brand

Open APIs in Financial Services For Dummies®, Red Hat Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-73568-7 (pbk); ISBN: 978-1-119-73570-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton
Acquisitions Editor: Ashley Coffey
Sr. Managing Editor: Rev Mengle
Production Editor: Tamilmani Varadharaj
Business Development Representative: Molly Daugherty

Red Hat Acknowledgments

A special thank you to Fiona McNeill, Rafael Marins, Hugo Guerrero, David Codelli, Emily Curley, Laney Badulis, Javier Leiva, and Roberta Ingham for their direct contributions to this book.

Table of Contents

Introduction

Application programming interfaces (APIs) inspire innovation and create new business opportunities. They slice through barriers to change by inviting more people to contribute to success and helping forward-thinking companies stand out from the competition.

To put it relatively simply, APIs are sets of requirements that govern how one software application can communicate and interact with another. But the truth is, APIs are far more than bits and bytes. The communication they enable make them front doors that automatically open to let new customers in. They're generators of new business and greater profit. They're also at the center of communities of developers whose aim in life is to collectively change the world.

And what's really changing the world is the concept of *open APIs*. An open API is a publicly available API that gives developers programmatic access to a proprietary software application or web service. Because it's open, any developer can borrow it and plug it into a project, making a connection that benefits all parties. In the past decade, the number of publicly available APIs has grown more than 50-fold.

About This Book

Open APIs in Financial Services For Dummies, Red Hat Special Edition, is your guide to this exciting world of opportunity. Whatever part you play in the financial services business of open APIs, this book puts forth valuable insights toward making it a successful venture. Far more than just a world for IT and software developers, there are vital considerations for those on the business side, for people involved in marketing, for risk and compliance experts, for the legal team. The key point is that APIs aren't just coding; they're products that must be managed and nurtured.

In this book, we discuss the basics about open APIs. We spell out what APIs can do for you within financial services. We discuss the security risks that open APIs can bring and how to mitigate them. There's advice on designing open APIs that can evolve. You find out how to make your APIs and development process easy and inviting. And you get a sense of the first steps the various players should take along the open API journey.

Foolish Assumptions

In writing this book, we've started with some basic assumptions about you, the reader:

- You're very interested in growing your business by tapping into the services offered by others or inviting others to automatically connect to what you provide.
- You oversee product development, or software development, or maybe marketing, perhaps legal or risk (many people have a hand in APIs).
- You'd appreciate a quick rundown on this exciting and innovative approach to business growth.

Icons Used in This Book

In the margins of this book, you may spot a number of icons. Each calls attention to important information in the adjacent paragraph.

REMEMBER

If you're reading through this book quickly, don't miss the especially vital information in this paragraph.

TIP

Here's a handy bit of advice for succeeding in the business of APIs.

TECHNICAL STUFF

The world of APIs does, in fact, revolve around software, which can be complicated. Here, we give you a techie tidbit.

WARNING

With every opportunity comes risk, and this paragraph points out how to prevent something from going awry.

CULTURAL WISDOM

These tidbits from Red Hat's ecosystem and customers give you words of wisdom about open APIs in financial services.

IN THIS CHAPTER

- Learning about APIs
- Discovering the API economy
- Understanding what APIs can do for you

Chapter 1
Why Use Open APIs?

If you're old enough, you may remember the days when computers talked to each other in beeps and screeches over analog phone lines. It seemed pretty cool and powerful at the time, but it was complicated and incredibly limited. Application programming interfaces (APIs) create an incredibly powerful way for systems and applications to interact with each other, and so much of daily digital life these days couldn't happen without them.

This chapter explores the basics of APIs, describing the differences between various types. It introduces you to the API economy and gives some specific examples of how APIs can take your organization to the next level.

Getting to Know APIs

REMEMBER

An API essentially defines the details of how applications communicate with one another, send requests, and get responses. In practical terms, an API spells out how a consumer can request the fulfillment of a certain service, exchanging data to send that request to a service provider.

For example, data is generated and processed by electronic devices such as your mobile phone, as well as the computer operated by your bank. Software applications that run on these electronic

devices generate, process, and exchange the data to make your digital banking transaction happen.

Software programmers build these software applications and their interfaces, such as your preferred digital banking application or your bank's online website. They use APIs to implement solutions for end-consumer applications, and they use APIs to establish other administrative services that require data exchanges.

Learning how APIs came about

An API is usually created to address the need of two parties that want to exchange data to request and render services. That request is transmitted across a communication medium from one party to the other. For example, consider the desire to purchase a bicycle from a bike-retailing website. A sequence of information must move back and forth between the web catalog and the browser on the smartphone of the person making the purchase.

REMEMBER

Business and technology experts define exactly what exchanged information will be needed to make this happen. They design an API that enables the transaction, using notations that computers can interpret for processing, and that humans can use to learn and refine the design. The API is essentially a protocol of common understanding for how the request and response will happen, involving the consumer of the service and the provider.

Now that this API has been created, it's used in software applications to access the services. As time goes on, the API will likely be refined to accommodate new requirements.

Understanding different APIs

The process described in the preceding section applies to any and every kind of API. But APIs differ in the way they're accessed and described, as well as by their purpose. Many APIs are created for specific users and cases and are quite customized in their design. Others are essentially open doors that invite everyone to the party.

The different types of APIs are as follows:

- **Open APIs:** These are accessible to people outside of the firm, and, if public, are APIs available for anyone to use, with no special permissions required. For example, there are APIs that take a location and determine the postal code for

shipping purposes. They can also be commercially viable, being used by other service providers and regulated by contractual agreements. For example, a retailer can request the delivery of goods to a distributor. The retailer and distributor have already established agreements for how such deliveries will work, and the API request includes some form of identity so the service can be fulfilled under the terms of the agreement.

- **Closed APIs:** Also called *private APIs,* these APIs tend to be limited in scope and used in exchanges between specific systems, like within the four walls of a bank.

Another way to look at the different types of APIs is to consider the format of data representation and type of protocols that they use. Data is represented in a particular way in an API that utilizes *Simple Objects Access Protocol* (SOAP). But in a *Representational State Transfer* (REST) API, data is represented differently. SOAP and REST are common API types for web applications, and there are others as well.

And then there is the general purpose of the API. Informational APIs request and deliver information, and such requests can be made many times without any actual change happening. Other APIs actually change the data between the party that calls and the party that responds to a service request. The result is some sort of a business transaction, such as a payment or a command to do something, such as ship a bicycle.

Exploring the API Economy

Most people have never really heard the term *the API economy*, but whether they know it or not, they're impacted by it. The concept of the API economy is really a way to illustrate the commercial activity that comes from adopting API technology. Think about the concepts of the *digital economy.* There wouldn't be a digital economy without an API economy. The API economy creates new services and functions — and not coincidentally, additional revenue opportunities can come from open APIs and data sharing.

When APIs are used to transform the state of affairs for businesses and end-users — such as by enabling an online purchase on a digital marketplace — that's the API economy performing its magic. APIs are used in many industries, from shipping to web retailing to other consumer applications.

Olivier Berthier of Moneythor notes that a digital customer is a more profitable customer. Open APIs are growing in importance as they provide low-cost distribution and commercialization across the supply chain. They're especially efficient for marketing, selling, and buying services and digital products. APIs are vehicles for growing a business via an ecosystem of partnerships. That's true for businesses that deal with digital products, as well as those that can operate mainly using software to manufacture, market, sell, and service their products or someone else's.

Imagine creating a web application that allows potential buyers to customize and purchase bicycles from many manufacturers. Software lives in the cloud, and open APIs connect several parts manufacturers. These partners share catalogs and prices to provide a wealth of options to bicycle retailers, who in turn can use the APIs to customize designs for specific customers through digital or web apps. You've just created a whole bicycle manufacturing and selling network that operates across the supply chain. And you've done so with no inventory and not a lot of capital expenditure. APIs are the secret sauce.

Indeed, the retail industry has used APIs for quite some time. Same goes for the travel industry. And Google APIs can be found nearly everywhere. Information is incorporated into everything from shipping and logistics to ride-sharing services.

What Can Open APIs Do For Me?

You could write an entire encyclopedia answering the question posed in that headline. Any and every industry has transformative uses for open APIs, limited only by the imaginations of their innovative minds. For the purposes of this book, which is considerably shorter than an encyclopedia, you look at just one slice of the business world: financial services. To put it simply, APIs provide a secure way for customers to access financial information, offering technologies that can share information safely over the

Internet with third parties. In the world of financial services, APIs are involved in these kinds of activities and attributes:

- Customer consent
- Customer authentication
- Security policies
- Transaction disputes
- Provider directory
- Provider operations
- Customer experience
- Data specifications

Read on to find out how open APIs can be revolutionary across a variety of financial-services industries.

Consumer lending

REMEMBER

Banks lend money at different terms and conditions, depending on countless variables. A fintech (financial technology) company can present consumers with a wide range of loan options by aggregating offers from numerous lender offers, adding in supplemental advisory services, and turning it all into an easy-to-consume online experience.

In this situation, open APIs are employed between the fintech operator and the banks to inquire and collate catalogs. The consumer ends up with a wide variety of options from which to choose. It's a win-win-win situation:

- Banks can reach markets they may have not be in before.
- Consumers gain a better selection and user experience.
- The fintech specializes in marketing and selling lending services without having to actually be a bank, and it doesn't have to service customers after the sale.

REMEMBER

Likewise, APIs can incorporate lending offers into the digital buying process, offering one-stop-shopping for buyers and giving consumer lenders a chance to expand the reach of their products. Take online car shopping as an example, in which buyers can search for a car, and then click a button to initiate the lending process. Another example: A vacation marketer can offer credit to

fund the travel right there on the same website. Such APIs allow lenders to come to the rescue at the point of need.

Retail banking

The most common use of open APIs in retail banking is for payments. The Open Banking Payment Service Directive Two (PSD2) emerged from regulatory laws in the European Union (EU). Under the law, a retail-banking customer owns her own banking information and can consent for third parties to see part of that banking data and initiate payment transactions on behalf of the customer.

The customer can then use a third-party service provider to initiate banking services, like a money transfer to other people, or businesses using one of the many bank's services, even across different banks if they offer better conditions or lower fees. In those jurisdictions with regulations associated with third-party data access — as in the case of PSD2 in the EU — some specific open APIs are provided by the banks by law.

Generally speaking, the world of digital banking used to be much simpler. Banks offered a single digital application with four or five key functions, and everything was self-contained within that single digital, online, or mobile application. Open APIs have expanded that world tremendously.

Think about your own digital life and all the digital touchpoints you use daily. You're using voice and digital assistants to initiate various transactions and perhaps signing up for financial wellness tools. These third-party applications need access to bank information securely. Open APIs make it all happen.

Asset management

REMEMBER

Asset management is fundamentally about fusing data from multiple sources together to make fruitful decisions and manage assets. Open APIs make it easier to share information inside and outside of an asset-management firm. Real-time information can flow across operating platforms and from multiple sources. The result is a more integrated experience for asset managers and customers alike.

Beyond financial assets, consider other kinds of assets that can be managed or controlled through API connections. Imagine, for example, owning a second car that can be rented out. The car can

be accessed once a code is sent to the controller in the car via the cellular network. Through an API over the web, the availability status of the car and its parking location are accessible, and the car can be located and rented via a digital app.

Insurance

Open APIs can provide many of the same benefits of marketplace described earlier. Aggregators can pull together insurance offers from multiple sources and connect with consumers, offering selection and easy enrollment. But that's just the beginning. For example, open APIs have been used to collect data from sensors on cars and trucks to enable usage-based pricing. And certain claims information can be collected from drones.

In the car-rental example in the preceding section, APIs connect with the insurance company to update GPS and accelerometer car sensor information. The result is a tailored bill for the driver. The driver is offered incentives to drive carefully, maintain speed limits, and avoid abrupt braking and accelerations, for example.

APIs allow the implementation of an automated and integrated process between insurance policy issuance and asset management. A technology company can orchestrate this business among several insurance carriers and car rental operations.

Wealth management

If you think about it, wealth isn't just holding assets in a single account or with a single firm. People have wealth spread across multiple firms and accounts. The best way to access this information is digitally.

The ability to aggregate all that wealth information into a single dashboard is quite attractive for wealth management customers and asset managers. Transacting across different wealth products and firms is also useful. APIs are the solution.

Corporate banking

The world of corporate banking has always revolved around data, and exchanging that data with customers has been paramount. Invoices, receipts, payments to suppliers — it all makes the world go around in this aspect of financial services, and that means information must go back and forth from the bank to the corporation constantly.

REMEMBER

Banks have traditionally had to set up complicated and costly systems to make this happen. With open APIs, though, they can now set up connections between new customers and the bank more quickly, easily, and cheaply, with no need for dedicated networks or complex infrastructure. These APIs send information in real time, giving customers an up-to-date view of liquidity in their lines of credit. Meanwhile, banking APIs for micro lending help small to mid-sized businesses decide who gets their lending business. That can optimize and automate cash-flow management.

Payment providers

Payment providers were among the early adopters of APIs in the financial services sector. Increasingly, APIs are now supporting additional event-driven interactions and channels, along with voice assistants. Open APIs ensure that payment providers can reach the devices and channels customers want to use for their transactions, and ensure that their services are adopted in a digital economy.

Payment providers can also provide tailored payment fees using APIs. Being able to offer dynamic pricing based on incentives helps them stay competitive.

IN THIS CHAPTER

- Looking at legal and compliance responsibilities
- Managing shared information
- Seeing the risks of APIs
- Controlling access and keeping information secure
- Stopping the exploitation of APIs
- Working through customer disputes

Chapter 2
Managing the Security Risks of Open APIs

Application programming interfaces (APIs) can be powerful, but risks are also involved when data moves around freely. This chapter explores the risks that come from dealing with APIs, the need to get the right experts to the table, the importance of collecting proper consent from customers, the ins and outs of keeping information secure and controlling access to it, the threat of cybercrime, and the ever-present need to deal with customer disputes.

Getting Legal Involved

Your innovative, entrepreneurial mind can dream up the powerful things your organization can accomplish through open APIs, but your IT teams need to figure out how to make those things happen. APIs are, after all, ways to conduct business, so the people involved in business operations are responsible for deciding whether to develop an open API and what to do with it. Your legal and risk management professionals think through all the things

that could go wrong, so you can build in the proper safeguards to steer clear of trouble. Indeed, the legal and risk/compliance teams need to have a seat at the table from the beginning.


TIP

Do an upfront risk assessment to allow all parties to strategize about potential controls that should be put in place. That kind of assessment doesn't just happen at the outset, either. You need periodic reviews as new data is available and regulations evolve. As time goes by, you build up experiences, and the landscape changes, your risk controls will need to be revised.

Think about the advent of digital banking. It has changed the world in dramatic and positive ways, for customers and for financial institutions alike. But these technologies also opened the door to potentially bad things that could happen if not for appropriate controls. When you're a bank, you have to be careful what doors you're opening.


WARNING

Open banking ecosystems carry all kinds of risks, and API development must consider such risks. Data breaches get the most attention, and no one wants to deal with the aftermath of an unintentional or malicious release of data into the wrong hands. Unauthorized payments can result from data breaches but also from malfunctions in systems. Then there are payments that are authorized but processed incorrectly or in an untimely way.

APIs must be able to support capabilities needed for legal purposes. For example, you need them to provide techniques to guarantee non-repudiation. You want them to have the ability to track API calls, uniquely identifying and auditing every single API request. That's always important, but particularly those requests that are transactional in nature, such as payments and authorizations for actions.

Spelling Out Legal and Compliance Responsibilities

Perform a risk assessment on both the data that's going to be exposed and the third parties that are gaining access to it. Your legal and compliance teams must provide guidance on customer data rights and the appropriate protections that need to be put in place. Pay attention to data rights because depending on the

jurisdiction, the consequences can be severe if those rights aren't respected.

REMEMBER

Your compliance experts must establish the text for legal assets, including all the terms and conditions for customers and third parties. They need to define legal protections for third-party use.

TIP

Consider APIs as contracts and API calls as potential transactions, and give them the appropriate legal considerations. Transactions, for example, typically must be protected by confidentiality and non-repudiation. And because your compliance and legal experts are advisers, they need to advise everyone else. They should clearly communicate your organization's liability related to open APIs. That includes reputation risk to all stakeholders.

Managing Customer Consent to Share Information

Managing customer consent to share information is where the regulatory considerations really start to become explicit. The General Data Protection Regulation (GDPR) was adopted a few years ago by the European Union (EU) and took effect in 2018, promising severe penalties for noncompliance. Among many other things, the GDPR spells out the important concept of customer consent.

WARNING

Customer consent must be gathered explicitly, with a clear scope for what it covers, such as accessing account information or making payments. And the duration must be clearly spelled out, too. Customers are also guaranteed the ability to manage their consent, and that includes the right to revoke consent and to be forgotten. With that in mind, the best open APIs need to include consent management capabilities in their digital applications. That gives customers the ability to control and adjust their consents.

The GDPR applies to anyone doing business with residents of the EU, but even if your organization has no EU connections, customer consent is a key in the API economy. APIs usually are paired with policies that guarantee access or specify types of data. It's a best practice to use an API management system, and not simply implement APIs via code.

REMEMBER

An API management system and a policy or rule system are essential for a robust implementation that guarantees and manages identities, governs automated activity, enforces security best practices, and handles entitlements. The code behind the API should focus on the business aspects, while the supporting systems will deal with security aspects.

Understanding the Unique Risks of Open APIs

What specific risks are posed by the use of open APIs? The answer varies from sector to sector, but it's informative to look at financial services and banking because this is one of the areas most impacted by cybercrime.

It almost goes without saying, but we'll say it anyway: The security aspects of banking APIs are paramount. A bank that exposes services through open APIs is opening fantastic new doors for customer service but is also potentially more vulnerable. By conducting business through the API channel, a bank can inadvertently introduce new forms of crime. For example, if payments are accessed via PSD2 APIs beyond credit cards and teller/ATM withdrawals, banks should integrate new procedures for funds availability across all possible channels.

Indeed, every access point poses a risk for financial information to leak out, and the anonymous nature of the Internet makes it all the more difficult. Early adopters of open banking have learned some lessons in this regard, sometimes the hard way.

WARNING

For example, criminals have tried to use APIs as a backdoor to access financial information on behalf of customers, through simple username/password combinations purchased on the dark web. This is known as *credential stuffing*.

Legitimate third parties can also be compromised through leaks of financial information. The posture of most financial services institutions is increasingly zero trust or trust no one, because mobile devices, third-party digital applications, and other access points all can be compromised.

Controlling Third-Party Access

Just because you're putting forth an open API doesn't mean all rules and controls are out the window. You're putting out a welcome mat, not throwing the door open to a wild party.

TIP

With that in mind, take note of these tips:

- Establish clear terms of use, including periodic auditing for compliance.
- Set clear policies and acceptance criteria for third-party onboarding (and these can be automated).
- Include clear steps for removing third parties (and automate this, too).
- Define mandatory controls that third parties must have in place with their applications.
- Perform periodic due diligence on third parties to ensure that those controls are in place.

REMEMBER

Third parties — such as an e-commerce website, other intermediaries, and the financial firm — have to ensure that customers' consent to process information during an API exchange is guaranteed only for the agreed-on purpose. That may be for specific products and services, or for specific time durations or geographical designations, or all of the above. A common authorization technique is the use of encrypted security tokens, which represent a digital form or declaration of permission issued.

Keeping Information Secure and Private

Securing authorized access to data and ensuring data privacy are paramount, and have technical, ethical, and legal implications. You must ensure that security policies are enforced throughout, from the source of transaction to the destination. Again, open APIs are a welcome mat, not a wide-open door. Before allowing access to data, you must require authentication through a trusted identity provider. Put in place strong authentication controls, perhaps including biometric authentication or using multifactor authentication techniques.

Ensuring and managing the identity of the parties involved is at the very foundation of a secure open API marketplace. In the API world, you're dealing with digital identities, and you need trusted super parties that can validate a digital identity as presented during an API exchange.

In practice, identity and security standards such as OpenConnectID are used in open API markets. You should ensure your technology provider supports the latest automation security practices. That includes using known and rated software stacks and protocols such as the latest encryption techniques, and OpenConnectID or OAuth for identity management.

Securing data in flight during a service request/response is a must-have requirement. You'll commonly do this via asymmetric encryption that transforms data before and after it is exchanged between the requestor and service provider.

By applying encryption and decryption techniques with agreed-on parameters, only the two parties are able to interpret the API data. This is a vital topic, but recognize that this is a big and complicated topic — whole books have been written on encryption techniques, secret management, and other aspects of cybersecurity capabilities.

Think about security management in the API world as if it's an onion. The various parties are sitting in the cores of distinct onions, dealing with all the multiple layers of the peel while needing to communicate with other peers who are sitting in their own onions. These onion peels are the layers of technology stacks and interconnected applications through which data is secured, communicated, processed, stored, routed, and filtered.

Continuously test and update the technologies you use to support the API economy. Also, keep your security professionals up-to-date on the latest knowledge of both vulnerabilities and remediation recommendations.

Open-sourced technologies such as the Linux operating system and security protocols like TSL and OpenSSL pose challenges similar to what APIs create. The experts in those fields have found that the best approach for maintaining secure systems is transparency, access to source code, and participation in discussion groups.

WARNING

Automating security patching is also quite important because most of the bad episodes that occur involve a software vulnerability that was known but not addressed and updated quickly enough. Consider the 2017 credit reporting breach that impacted data for more than 140 million customers. It involved exploiting a software bug that was disclosed two months before the attack happened.

Monitoring and Auditing Access

APIs for commerce should be always backed by an API management system. The system maintains policies for security management, while managing and tracking the life cycle of every API.

REMEMBER

Monitoring and auditing should be part of the API management system instead of being implemented ad hoc by applications that support APIs. That's because controls, monitoring, and auditing should be managed independently from the asset being managed, which in this case is the application that uses APIs.

Be sure to establish third-party reporting, including suspicious activity reporting. Ensure that you tag transactions so that you know what and where the source is. These days, access information is increasingly provided to customers, too, so they're also aware of access and usage.

Stopping Bad Guys from Exploiting APIs

Not to be too much of a downer, but criminals can't be stopped. They're criminals, after all, and many of them are incredibly smart and always looking for ways to take advantage of the anonymous nature of the Internet to commit crime. Your objective is to put reasonable safeguards in place to stay a few steps ahead of them, including multifactor authentication that makes it difficult to exploit open APIs.

REMEMBER

As the API management system monitors every aspect of any API exchange, you're able to detect and remediate patterns of attack or improper use. API calls should always carry a form of identification and authorization token, and usage policies are vital. The management system is integrated with other systems — the outer

peels of the onion — which usually handle lower-level security such as communication security.

Handling Customer Disputes

Third parties and customers both need you to establish a way to manage disputes. The United Kingdom has been a leader in this area, establishing a dispute management system to cover all participants involved in the open banking scheme there. If the market doesn't have a mechanism in place, it's still a good idea for individual firms to have a public mechanism for handling and managing disputes (ideally in digital form).

Note that credit card issuers and networks provide dispute management as a service, because they know disputes will happen involving the merchant, the payment processor, and the customer. The systems they have in place help mitigate risk for the firm and the customer alike, and boost customer confidence.

APIs sustain business beyond the data exchange, involving legal entities behind the APIs. The location of electronic business is virtual, but jurisdictional forums are associated with the legal entities, and those can operate in one or many territories. It's important to establish legal agreements with the legal entities behind the APIs and follow all local laws.

It's normal to have parties needing to accept one-way or mutual agreements, often involving the exchange of digital API keys. At a minimum, the API business must honor nonrepudiation — establishing assurance that the sender of data gets proof of delivery and the recipient gets proof of the sender's identity. That way, neither can later deny having requested a service via an API invocation.

IN THIS CHAPTER

- Assigning responsibility for the API
- Making headway in the API ecosystem
- Considering the characteristics of a winning API
- Preparing the API for change

Chapter 3
Designing Open APIs for Change

What does it take to develop application programming interfaces (APIs) that are game-changing today and ready for tomorrow? A lot of forethought and attention to detail. Involve the right people to ensure the API serves its mission at the outset and evolves as needed as times change.

This chapter explores who "owns" the API within your organization, what attributes are essential to succeed, and what considerations you must give to performance. The chapter spells out details that architects need to ponder, and examines what might cause the need to revise your API later.

Who's In Charge of APIs?

They're a bunch of computer coding, so it makes sense to think of APIs as something that is within the bailiwick of the IT department. And that assessment is not exactly incorrect, but it is incomplete. Indeed, APIs are much more than simply information technology assets. There are legal considerations and compliance concerns (we cover those in Chapter 2). And as important as anything, there are business aspects, because APIs are opening the

door to whole new ways of operating, new revenue channels, and new customers.

REMEMBER

So, it's a mistake to think in terms such as "IT owns the APIs." Successful APIs businesses have thrived because APIs have been treated as full-fledged products. In that regard, they're given widespread attention from the beginning of the go-to-market process, including marketing research, competitive and cost analysis, marketing, and ongoing operations.

If you think of APIs as full-fledged products, then, it makes sense that they're "owned" by product management. That team works in close collaboration with both IT and business stakeholders.

A related discussion involves who owns the data associated with open APIs. That depends on the specifics. APIs frequently carry business information, such as product SKU numbers, prices, and quantities. That kind of data belongs primarily to the operational business units, such as the procurement and accounting departments. There is also other data that's more technical in nature, such as security information. That kind of data is managed by the IT and operations departments.

Succeeding in the Ecosystem

What does it take to succeed in the API marketplace? There are a couple of key starting points:

- The API must be easy to find. Success depends on marketing the API to attract appropriate consumers.
- It must be easy to use and well documented, inclusive of examples.
- It should have an active community behind it, allowing interested parties to discuss what works and what doesn't.

WARNING

That last bullet point is an important part of the API product roadmap. Without a feedback loop and a product management team paying attention to it, the API can easily wither and die, as software developers quickly turn to competing digital options.

Increasingly, there are standard schema definitions for data elements, such as UK CMA, Berlin Group, BIAN, and ISO 20022. Pick

relevant standard definitions for your API, and you can help promote interoperability inside and outside of the firm.

Focus on security interoperability first and data second because data contracts are driven by the need of your partners. Also, keep in mind that standards will continually evolve. That means you must perform periodic reviews of standards, and keep an eye out for emerging or new standards.

Ensuring Performance, Availability, and Resiliency

Consider this scenario: You offer an API to buy volatile assets, with prices that vary frequently. If the API can't respond quickly and process orders rapidly, competing customers may snap up the inventory at the requested price. For this kind of reason, brokerage houses buying and selling on the stock exchange must move quickly. If an API doesn't make a deal happen as requested, it has failed in its job. Lengthy API roundtrips — that's the elapsed time between request and response — will create frustrated customers.

Fast response is, therefore, a key performance indicator of a good API. And good technology is only part of the story when it comes to strong performance. Indeed, you can't defeat the speed of light, which is an absolute upper limit of signal propagation over network media. Certainly, signals can move quickly, but sometimes not quickly enough, especially when there's considerable distance between the requestor and the service provider.

A practical test from your computer is using the *ping* command, which gives you an average roundtrip time of a communication to the service or API provider, usually in milliseconds.

TIP

There are several ways you can mitigate delays. For APIs that request information, also known as *queries,* the service provider can use information kept in memory. Such caching techniques avoid delays associated with retrieving data from slower databases or other systems.

APIs that are part informational and part transactional can adopt Command Query Responsibility Segregation (CQRS) design. That sends queries and transactions to different systems that are all optimized for best performance.

REMEMBER

API management allows you to route different API requests to appropriate subsystems. That boosts performance and, even more important, availability and resilience, usually by adopting redundancy of the systems that serve APIs. Batching many API calls into one is also a common technique allowing better throughput.

The bottom line to consider is slowdowns happen. So expect them. One way to anticipate and deal with performance slowdowns is by implementing a circuit breaker to monitor for failures. Sidecar tooling (like a service mesh) can also ride alongside an API — collecting throughput data to continuously monitor performance and speed — and is foundational to forecast potential bottlenecks.

What about an API that supports a lengthy process, such as a request that requires an escalation to a human being for further acceptance? Well-designed APIs return a response indicating acceptance of the request, then follow up with a second transaction confirming completion of the request.

This common behavior occurs in business and in life, where events and activities are often correlated but asynchronous. Email, text messages, and voicemails are common examples of such asynchronous exchanges.

Characteristics of a Well-Designed Open API

REMEMBER

A well-defined API is intuitive, easy to understand, and easy to use. With that in mind, designers spend extra time to minimize the pieces of information requested for each API. They may provide a main API that's core to the business and secondary or auxiliary APIs designed for specific use cases. They may also be to ensure high performance or to carry over operational and support exchanges. This section gives you additional, specific considerations.

What architects need to know about security

Industry trends and regulations governing the marketplace usually inform the security techniques and protocols chosen for APIs.

Business architects aren't as concerned about this area, as their focus is ensuring APIs exchanges take care of the various business functions and carry the adequate data needed to support those functions.

The security architect is responsible for aspects related to cybersecurity, identity management, authorization, data security, and privacy. Security information carries identity and purpose of the business-related API requests throughout the system, so it's important to have collaboration between the two areas. Businesses processes must verify the legitimacy of an API transaction request.


TIP

There must be standardization on access tokens. Architects then must put in place the technologies to authenticate and authorize end users, with the help of these standards.

What architects need to know about data


TECHNICAL STUFF

JavaScript Object Notation (JSON) and Representational State Transfer (REST) are ways to represent data and design APIs. Designing a REST API requires knowledge of web architecture and REST architectural principles. That means, for example, choosing the right mapping APIs to connect the REST verbs — such as GET, PUT, HEAD, and DELETE — with the part of the system responsible for queries and for transactions.

What architects need to know about schema

Schemas define what data is expected in a request, as well as in the response. A software engineer or a database engineer must know how to model data objects and apply data normalization techniques. What's especially important is being able to model errors and exceptions, which describe abnormal outcomes of requests and responses.


TIP

Architects must apply DRY principles ("don't repeat yourself") and keep definitions concise, and avoid unnecessary nesting and wrapping. Reuse standard definitions for data, exceptions, and security policies and include reasonable documentation.

What architects need to know about cloud technologies

There's a whole lot to know about cloud technologies, but for these purposes the most important point is that they make it easier to release services which are independently deployable and scalable. You can, in fact, run multiple integrations side-by-side.


TIP

Cloud technologies help enable such concepts as blue/green deployment and canary releases. Both are ways to reduce the risks inherent in new releases. The blue/green concept establishes two nearly identical production environments, so that when you switch to one of them, you can quickly flip to the other if something goes awry. A canary release calls on the coalmine metaphor by first rolling out a change to a small subset of users to be sure everything is okay.

What architects need to know about buying open APIs

Buying open APIs isn't unlike getting into any new area or product sector through acquisition rather than organic development. You get to market faster, but you lose control of the evolutionary process. One approach is to buy for parity and build for competitive differentiation.

Many times, APIs are a commodity, and they're increasingly included with packaged platforms. Be sure to clearly establish performance and availability expectations, and insist on performance reporting along with invoicing. Establish commercial rebates in the event of missed service levels.

Dealing with Change

Businesses must adapt to market needs and make changes quite frequently. On the other hand, foundational business services such as inventory management, fulfillment, and pricing have not significantly changed for years. Successful new businesses thrive by creating distinctive offerings for end customers, but it's quite helpful for them to reuse already existing and popular foundational business services such as customer services management, support management systems, and human resources.

TIP

For these areas, APIs make it possible to provide and consume value. New businesses can tap into such helpful resources as Salesforce, ServiceNow, and Workday services through their respective APIs. The more organizations can reuse and recombine foundational APIs and services to build offerings, the better their ability to deliver excellent products and services at a lower cost.

Modern API-fronted business services are cloud-native, which means they can run in a cloud environment. Cloud-native services are usually packaged and distributed in the form of containerized software, which include all functions needed for the business service to operate. Think of containerized API-fronted business services sort of like independent and reusable building blocks, which can be reused and combined to create all sorts of amazing solutions.

What causes the need for revision of open APIs?

REMEMBER

Changing regulations governing various businesses can make it mandatory to revise open APIs. Banks, for example, spend a large part of their upgrade/update budget complying with new regulations. As new laws and regulations emerge, open APIs must respond with additions or modifications.

Changes in business performance also can drive changes in APIs. Competition can spark the need, forcing changes in specialization, or the addition of new service options at different price points. As with any product, as the market changes so will the API. But with APIs, if the contract changes between parties exchanging the product, the APIs need to correspondingly be adapted.

Accommodating evolving API standards

REMEMBER

It's often necessary to support multiple versions of APIs because not all participants are able or willing to update their systems. The technology supporting the APIs — often referred as the API management system — must be able to manage multiple versions of APIs and associate each API version to the specific supporting system.

What's the long-term vision?

There's no question that banks and other organizations will use API-enabled services more and more in the future, sometimes through third parties and sometimes within the organization itself. Deciding who provides the API will depend on cost per service and compliance.

TIP

Choose industry-standard APIs rather than proprietary APIs. That way you're procuring services in a healthy, competitive market with lots of players and the ability to quickly change suppliers. The result will be the best service at the lowest possible cost.

To use banking as an example, standardization of banking APIs was the result of an initiative led by the Banking Industry Association Network (`bian.org`) and ISO20022. It resulted in a clear definition of reusable modular business services that can be purchased or rented, then quickly recombined to adapt business offerings.

IN THIS CHAPTER

- Knowing what makes your open APIs stand out
- Building trust with developers
- Solidifying partnerships
- Looking at pricing
- Knowing how to measure success

Chapter 4
Making It Easy and Inviting

Partners are not just technology suppliers — they need to be treated as first-class citizens. To win business, you need to make the benefits of joining the ecosystem clear, and make it easy for partners to get onboard.

This chapter offers suggestions for letting the world know about your application programming interfaces (APIs) and winning the hearts and minds of developers. It discusses what goes into a good partnership, and spells out strategies for establishing pricing and measuring your success.

Making Your Open APIs Stand Out

You're in the marketplace for APIs. So how do you reach your potential customers? How do you make your product stand out so that it gets attention and, ultimately, is chosen for use? This is where your organization's venture into open APIs is far more than simply writing code. The answers have everything to do with the business considerations.

CULTURAL WISDOM

Consider the wisdom of Paolo Sironi of IBM when thinking about your business considerations. Sironi explains that banks facing higher uncertainty can excel in extreme digitization only if they embrace openness (open banking), become transparent (to generate client trust with data on digital platforms), and deliver client value through human advisory relationships (elevated by artificial intelligence [AI]).

REMEMBER

Your API should reflect the language and the dynamics of the business in which your target audience is involved. Understand the pain points that can be addressed through API-fronted services. Those who connect with your APIs are software developers and business sellers, such as distributors, and these people drive your business.

Developers typically seek information from peer industry discussion groups and software repositories such as GitHub, as well as known vendors. Business sellers are usually interested in vendors or partners that can grow their markets and make their sales happen faster.

TIP

In fact, APIs often falter if there isn't an active user discussion group, along with documentation and coding examples. Venues where digitization is the topic of conversation are excellent places to introduce digital forms of business driven by APIs. Innovative companies will even choose to show code snippets of the APIs they're offering, right there on their main web pages. They know capturing the attention of developers is key, and what better way to do that than with bits of code?

Winning over the Developers

Developers love code, and they're quite fond of open source because it provides comfort that there's a community of users with whom they can exchange information about your APIs. They want to see the software artifacts without restrictions — this form of transparency builds trust that eventually creates loyalty.

TIP

With that in mind, follow these suggestions:

- Provide plenty of examples of code, easily accessible without need to gated access. A one-time signup process is enough to track the developer usage on your digital property.

- Make it easy for developers to get started, with easy-to-understand guides based on real-world examples and samples related to using the APIs.
- Listen and respond to feedback, and don't skimp on marketing and outreach, because developers need to know you exist.

Building Partnerships

If your business provides or consumes services through APIs, the best partners are the ones that are already familiar with APIs. These organizations are already thinking digitally and already sold on the value of power exchanging data and services in an automated fashion. Depending on what kind of business you're offering or consuming — distribution, marketing, or sales, for example — partners may operate in different market niches. API standards associations offer a fine place to start to look for players.

TIP

Look for partners that extend your value chain. For example, if your business is financial services, seek partners that have a natural affinity for the financial services products you provide. If you provide auto loans, seek connections with digital auto marketplaces and other auto sellers.

Increasingly, leaders are creating their own incubators to facilitate collaboration and co-development, or using third-party services to create challenges that end up recruiting partners. Barclays, for example, offers Rise, which fosters connections in the fintech world. And HSBC partners with T-Hub on an accelerator program that has a focus on creating commercialization opportunities.

Here are some key questions to ask about potential partners:

- Do they provide value to your customer?
- Do they extend your reach as an organization?
- What's the potential direct commercial value?
- Is the potential partner trustworthy?

What is your partner looking for?

REMEMBER

Your best partners share your values and complement your business. An exceptional partnership is one where both parties are trying to determine how joining forces can help conquer a wider market. That's the sign of a partnership that's strategic and less speculative than a partnership that's simply selling and buying from each other.

Certain standard service capabilities are expected in a partnership. These include the usual service level agreement factors, such as service availability, quality, and performance. Nevertheless, a solid partnership goes beyond that. Partners will look for the ability to quickly respond to changing needs. Increasingly, leading API providers have been asked to provide testing suites and certification kits to make sure third-party applications work appropriately with the APIs.

Can partnerships help you build APIs that evolve?

As your business grows, you may want to expand into new areas. If you choose to partner with companies that have an active network of partners themselves, that creates a multiplicative effect, which you'll recognize as the power of the network.

Your API catalog is the entry door of your digital business. You can grow by adding new APIs/services for your customers, which may be then served by your partners. API-savvy partners are usually happy to let you reuse their APIs for your customers, thus extending your API catalog.

REMEMBER

Partners can also bring new needs, which can serve as a catalyst for innovation with your open APIs. Without truly connecting with consumers about the usage of your APIs, you run the risk of providing capabilities that no one really needs or wants, or missing capabilities that could make your APIs more useful.

Setting Pricing

An API is a means for facilitating business that reflects the services or products rendered behind the API. As such, you may not be able to monetize an API by itself. However, when partners and

customers are increasing API commerce with you, it makes sense to set up tiered fees at the API level, depending on the business volumes the various partners and customers drive. It's generally a best business practice to offer volume discounts.

REMEMBER

API management systems such as Red Hat 3scale API Management allow you to set pricing, generate show-back and charge-back reports, and create bills for customers and partners. Such API management systems have APIs of their own that allow you to track usage and change API fees for specific users in a programmatic and precise way. You can easily create and maintain sophisticated pricing schemes, such as dynamic pricing.

TIP

Always have a free tier for evaluation. And remember that revenue generation isn't necessarily the right business model for every API.

Many financial-service firms have started by offering their APIs for free, either by mandate or to acquire market share. That said, a tiered pricing strategy is useful as firms begin to think about monetization (and "free" can be a tier). This kind of strategy also allows for higher discounts through greater utilization, or vice versa, depending on whether your objective is to expand market or grow revenue.

Some organizations have adopted profit-sharing models, sharing in the wealth when volumes are increased. Various kinds of incentives and special offerings can be built, with associated terms and conditions connected to the business conducted via API.

Measuring Success

TIP

A simple count of the number of active partners and relative volume of API calls per partner offers a snapshot of the business generated through your APIs. Another important metric is how many distinct APIs from your catalog are utilized over time.

Other measures can give insight into usage, such as the number of live products that use your APIs, and how many end customers renew their consent, and of course, such aspects as the costs of API services and ultimately revenue.


TIP

With these measures, you can get a good sense of the success of a specific API. Just monitor the increase or decrease in frequency of use, as well as changes in the number of distinct customers using a given API. It's also important to track errors.

Then there's the value of benchmarking. Advisory boards and surveys of the community can give you a sense of how you're faring.

IN THIS CHAPTER

- Choosing to build or to buy
- Charting the API life cycle
- Testing, maintaining, and retiring APIs

Chapter 5
Creating It Smartly

Like so many initiatives, creating and marketing open application programming interfaces (APIs) can be done in many different ways, and it's not like one way is right and another is wrong. Still, there are smart, best practices that are worth considering.

This chapter goes down the path of creating APIs in a smart and effective way. You explore the question of whether it's better to build your own API or buy someone else's. You also discover development teams and community development and delve into the API life cycle — how it starts and ends and what happens in-between.

Deciding to Build It or Buy It

Consider that a well-designed API results from the work of business and technical architects. However, what if your team has no previous experience in building and maintaining an API? The most appropriate course may be to use a third-party API. On the other hand, if you choose to build your APIs and you have the capabilities in-house, there may be guidance from a well-established standards body.

TIP

Situations definitely exist when it's worth considering buying an existing API. For one thing, it can greatly shorten the time to market. This is an especially worthwhile approach for APIs that represent non-strategic business, such as secondary supporting functions, that also have low or zero company intellectual property.

On the other hand, if it's a case where the API represents your distinctive business competency, then building is usually the best choice to maintain a competitive edge. That, of course, requires experience and collaboration from both the business and technical teams.

CULTURAL WISDOM

Eyal Sivan, also known as Mr. Open Banking from his podcast of the same name, confirms this collaboration. He notes that to be successful in building an open API platform, functional teams need to be brought together, made up of a combination of business and technology stakeholders. Teams need to go beyond traditional silo mentalities and work together in an environment of collaboration and sharing to successfully move forward with open banking. Check out Mr. Open Banking at `www.mropenbanking.com/about`.

TIP

To help your team build and maintain the right skills, you may wish to formalize skills training, including in emerging technologies. Also, create and promote opportunities to move between teams and roles, and establish a mentoring program. All are tried-and-true approaches for getting the right talent on your team and retaining your team with interesting work.

Another approach is community development. That's a good way to tap into a broader pool of talent. But you must establish clear goals and objectives in the developer community, and create clear contribution guidelines. Extend APIs as a product principle and identify community maintainers or stewards that will keep watch over standards and review contributions.

Innovative companies such as fintechs often choose to contribute building an API in a community forum, involving other parties and following an open-source approach. This helps ensure the relevance of the development, and grows maturity in a market niche. APIs in a community are a form of initial market,

where players can choose to provide best implementations of business offerings behind the API, either in a proprietary or open source way.

For a great developer community, recruit like-minded organizations to contribute. You have to give a little to get a little, so invest in "seeding" the community. Make it easy to make a solid contribution. Building with a blended delivery team has both operational and test considerations during the construction process. You can improve delivery and deployment speed through automation. And increasing collaboration can often uncover new levels of innovation.


TIP

When it comes to building your API in a smart way, look to the cloud. A cloud strategy promotes consistency across environments, which means you're less likely to get "works here but not there" problems. In addition, cloud technology keeps your focus on code rather than infrastructure, while enhancing portability and maximizing scalability.

Charting the API Life Cycle

A typical way to start and maintain an API initiative is to share early and often, and experiment in a community to refine requirements. Set API roadmap milestones to distinguish work in progress and experimentation with stable versions and releases. The community-working group usually defines the maturity stages of the API.


TECHNICAL STUFF

A schema — such as JSON, XML/XSD, and OpenAPI Specification (OAS) — usually represents APIs. Representations can be compared to monitor changes.

As for marking the finish point, recognize that APIs are software interfaces, so major and minor releases mark the end of subsequent waves. API versioning and related documentation of change are common approaches. Define the concept of API deprecation for a given version of an API. An API is deprecated if it's considerably redesigned or the business and vendor parties no longer support and maintain old versions.

Testing, Maintaining, and Retiring APIs

There are several tools for testing APIs. To begin with, well-defined APIs include in their definition what outputs are expected from given inputs. This allows you to automate API testing. Other software tools and libraries, such as Generator, can generate code to call and to serve an API. This allows building test suites.

APIs should be considered full-fledged products. As such, you should follow product management best practices regarding evolution and support. One reason some projects fail is that the organization considers an API an extension of the code that's built once, instead of viewing it as an ever-evolving product with a dynamic nature.

That's not to say an API lasts forever. The API represents the business behind it, so when the business is no longer profitable, the API is usually deprecated and then discontinued.

Keep a minimal form of API responsiveness up and running for a while even during the discontinued stage. Proper error codes will indicate the API is no longer operating. That allows customers to take appropriate actions without creating major disruption at the software integration level.

REMEMBER

Like everything else, software should evolve. Keeping old APIs and methods can make the service unnecessarily complex. If you think otherwise, you may be tempted to put everything but the kitchen sink into an API, trying to anticipate future needs.

Don't write code that you think you might need in future, but don't need yet. Write less code, and then evolve when appropriate. Be sure to give consumers time to change over when the time comes.

IN THIS CHAPTER

- Making the business case
- Preventing trouble
- Fulfilling the requirements
- Making connections
- Getting things done

Chapter 6
Planning Your First Steps

You know that quote about "it takes a village?" You could say that about application programming interfaces (APIs), too. Many players have a hand in succeeding in the world of APIs because they affect not only how IT works but also how connections are made and how business is done.

This chapter looks at some of the first steps the various players on your team need to take as your organization heads down this exciting path. The product executives must make a business case, while risk and compliance professionals are on the lookout for trouble. Architects, partner communities, and engineering managers all have their vital roles.

Product Executives: Making the Business Case

Open APIs facilitate connections with new customers, but you need to make a solid business case of how your API provides benefits. APIs represent the way to access and market business as a service model. Consider financial services as an example of how this can work.

In the API economy for banking — sometimes referred to as *open banking* — the path to success demonstrates that you can sell your products and services by way of others, typically distributors, aggregators, and fintechs. This happens by

- **Achieving lower cost of sale per product unit:** This means lowering the bottom-line cost.
- **Reaching wider markets and white-space niches by the means of others:** This is all about increasing the top-line revenue.

Decreasing friction


TIP

Measure the sale cycles timing via API channels, compared with what it's like employing traditional non-digital methods. Through APIs, you can potentially automate the whole process of moving a sale cycle from request for information, to request a quote, to purchase order, to fulfillment. In that way, APIs offer streamlined access to information and the implementation of the entire process in a shorter time than the competition. That's what you call lowering the friction in conducting business.


CULTURAL WISDOM

Dr. Roland Folz of Solarisbank confirms these possibilities. He states that customer-centric servicing today means reducing the number of clicks you have to make, which minimizes inconvenience and moves money faster. This process demands the seamless movement of data within an ecosystem and open APIs that are part of an integrated banking platform.

Reducing churn

Your API management system monitors how many new customers apply to your marketed API business plans and the business activities. Monitoring increasing versus decreasing onboarding and other activities provides your organization with immediate measurement of business performance. Monitor both qualitative and quantitative aspects. Net promoter score qualitative measurements of digital sales are widely used.

Reducing risk

Open APIs enable lower cost of entry to new markets, particularly by way of the partner network. The more markets you're

in, directly or indirectly, the more diversified you are. And that reduces your competitive risk. What's key is how you follow through from API-initiated business transactions to rendering services or delivering products to customers. Electronic businesses can introduce new risk, largely related to cybersecurity and identity management.

Risk/Compliance Professionals: Preventing Trouble

With APIs, your business is extended by others, and that's by design, of course. However, as others partake of the gains, they also are exposed to risk.

Taking control

Good education among project participants helps to build a common understanding of the potential risks. And it puts developers in the right mindset to design and build for security from the beginning. The more you can push security into the platform on which you're developing APIs, the easier it will be to maintain governance over your ecosystem. Make sure risks, controls, and standards documentation is available and also easy for appropriate parties to understand and update.

Tracking compliance

If you have a good measure of your API business to form a baseline that allows you to later on estimate the deviance from the current state. As new rules (or misbehavior of a partner) force a new level of compliance, you monitor it. Having fine-grained controls on API usage reduces your exposure to noncompliant behavior.

Keeping an eye out

What should risk and compliance professionals be asking about and looking for? For starters, changes in API usage patterns. Some of them are natural, as they reflect changing business conditions across the supply chain. But others could be red flags indicating unexpected or fraudulent usage.

TIP

Ask for transparent reporting from your partners. And provide administrative and backup channels for communication with you regarding potential compliance or risk concerns.

WARNING

Compliance monitoring is a way to watch out for risk. A zero-trust posture is always good practice. You must constantly monitor how your partners are using your APIs. You can do this by fronting an API service with an API management system, to apply risk-reducing policies. For example, it can throttle or limit API calls per partner, as defined by the business contract. Monitoring APIs isn't enough. You must consider underlying business impacts as API calls increase. Cumulative credit and cash flow are examples.

Architects: Fulfilling the Requirements

For regulatory-driven API initiatives, the regulatory body usually issues rules for API capabilities and responsibilities. In some cases, though, API specifications aren't available, which gives the implementer freedom to define them. For nonregulatory-driven API business, there's often some type of consortium established by members that have a common desire to form the new API-based market.

Finding authoritative information

The source of truth varies by sector. In the banking sector, for example, central banks or government agencies are usually the authoritative source. Many regulations may apply to API services, including rules governing generic business practices and data privacy. Business consulting companies specializing in risk and compliance are good resources for obtaining guidelines and recommendations.

Avoiding penalties

What happens if the applicable requirements aren't met? Regulations typically include indications of the consequences of noncompliance. Potential risks — both external and internal — exist for the business. For those who want to know what the impact is, the organization's risk officer should have a good idea.

Community or Partner Managers: Making Connections

In many cases, the best way to make your open API a winner is by connecting with an active forum or community. So how to you find partners with the right capabilities? Groups of people representing different organizations usually establish forums for market-driven API initiatives. Some groups are open to everybody, while others require subscriptions to access documentation or to participate in working group discussions.

Not surprisingly because this is all about online business, there's typically a forum website, so searching the Internet is a good place to start. Your initial source of information at any specific company may be the chief digital officer.


TIP

Your early activities in this area may include building a website with documentation and examples of API usage. Open-source projects will typically share APIs and example code for trying out. A source code repository such as GitHub or GitLab is ideal for this kind of sharing.

Engineering Managers: Getting Things Done

Engineering managers are among those doing the heavy lifting when it comes to the technical side of APIs. Among other things, they must meet the project objectives and ensure there are detailed enough requirements to get it done.


TIP

Elements and verbs of the APIs have to be detailed enough for the set of integrated systems behind the APIs to carry on the business function and granular enough to enable reuse of API componentry. For guidance, look to the S.M.A.R.T. principles — simple, measurable, achievable, relevant, timely defined.

Setting the deadlines

APIs reflect the digital integration aspects of business among participants. There are two main aspects: the API life cycle, including phases of API design and testing, and the implementation of the business functions behind the APIs.


TIP

Have the API defined as early as possible and available to partners for testing. You want to define the API and have a system available that responds to the APIs, even if it's just a mockup of the real business.

Modern agile project management techniques set sprints that can be as swift as couple of weeks. Development teams should strive to have initial APIs up and running sprint by sprint and define timelines to have the business processes behind the APIs ready in phases, starting with the primary API (which may be a login).

Defining the budget


REMEMBER

The size of the budget depends on the purpose and scope of the APIs. If products, services, and related processes are already present in the company, then the project mostly entails building the appropriate API-supporting IT services and the associated integration. A starting point for costing is to define the hardware and software infrastructure requirements.

Establishing requirements

Feasibility is mostly related to the presence of digital product/services, related business processes, and personnel skills. Business architects and analysts define the business requirements and discuss them with software architects and developers. This is usually done in recurring interactive sessions that define the list of activities required to implement the APIs.

IN THIS CHAPTER

- Understanding APIs and how they're different
- Charting early API success
- Learning the advantages and drawbacks of open APIs
- Evolving your APIs
- Looking ahead to the future of open APIs

Chapter 7
Ten Q&As about Open APIs

Maybe you've read the whole book to get to this point, or maybe you jumped here first. Either way, here we compile key points, questions, and answers for easy consumption:

- **What's an API?** APIs describe how one software app communicates with another. An API is a set of requirements governing the communication and interaction between different apps. Check out Chapter 1 for more info.
- **What makes open APIs different?** An open API is no different than any other kind of API, except for the fact that it's published on the Internet. For more on types of APIs, see Chapter 1.
- **Who owns APIs?** Consider product management as the owner, collaborating with the IT and business stakeholders. APIs are products, and someone has to think about the whole product life cycle, all the way back to the initial market research. See Chapter 3 for more.
- **What's an example of early success?** An example of how APIs can work belongs to eBay. Like every other popular place on the Internet, its content was "borrowed" or "curated" from other places. The company decided to offer APIs to provide

access to data. eBay plugged into more ecommerce, and businesses listed products through eBay and used the APIs to market those products through their own websites.

- **What are open API advantages?** Open APIs fire up the creativity of the global coding community. A company, for example, can build on an existing app, dreaming up some new functionality, and use APIs to share the new capability with others for new revenues. See more details in Chapter 1.
- **Do open APIs have drawbacks?** Yes. The biggest is that if your third-party company taps into open APIs, you're vulnerable to subsequent decisions by the developer of that API. If that developer changes the terms of use, anyone using that API has to comply. See Chapter 2 for more on security and Chapter 3 for more on change.
- **Where are open APIs stored?** The code resides in a developer portal, which is attractive to other firms' business models because these portals exchange data that can unlock the power of open innovation. Open APIs are listed in a catalog through the portal, documented and ready to be part of the development process.
- **When do open APIs need to be changed?** The need for change can be sparked by regulations or because the organization wants to create a new business dynamic or more sophisticated offerings. As changes happen, APIs need to be adjusted. See Chapter 3 for more info.
- **What are the alternatives to open APIs?** You can conduct commerce without using APIs, instead using technologies such as proprietary VANs, file-based batch exchange, X12 or Edifact messages, or legacy application protocols.
- **What's the future of open APIs in financial services?** Expect the transformation of banks to interdependent ecosystems. The contract-first approach, validated by the open API specification, is just the tip of the iceberg because it covers just one type of interaction connectivity. There's a rise in the implementation of similar solutions for event-driven architectures in which similar information is required (such as endpoint information, subscription destinations, and the most important part, the data payload schemas). Ultimately, the most successful banks are likely to shift away from building full end-to-end financial solutions and toward assembling best-of-breed financial services by using a number of ways to connect across ecosystems.

Red Hat

Build for change

Use your technology as a strategic asset with Red Hat—and lead the market by exceeding customer expectations.

Learn more at **redhat.com/financial**

Create opportunities with open APIs

Application programming interfaces (APIs) inspire innovation, bridge agility gaps, and create new business opportunities for financial institutions. As competition increases within a more digital world, open APIs help embed financial services into the day-to-day lives of customers. Open APIs open a world of possibilities. Whether you're on the business side or hands-on keyboard, this book leads you through what open APIs are, why you need to understand them, and how to get started.

Inside...

- Top ten Q&As about open APIs
- Choosing to build or buy APIs
- Understanding the API life cycle
- Making the business case for open APIs
- Succeeding in the API ecosystem
- Properties of a well-designed open API
- Measuring success of your open APIs

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-73568-7
Not For Resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.