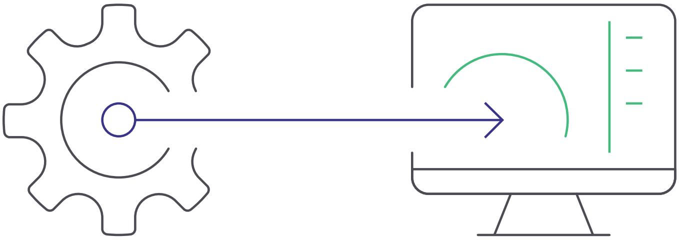
Duck Creek
Technologies

The P&C SaaS Core Systems RFP:

7 Questions Every CIO Should Ask the Vendor

Table of Contents

Introduction



Core system purchases are critical decisions carriers must evaluate from a number of dimensions.

Imagine this scenario. Your Head of Underwriting, Head of Commercial or Personal Lines, Head of Claims, etc. has been in discussion with several software-as-a-service (SaaS) core systems vendors to solve one or more specific business challenges: maybe it's a desire to pivot into new lines of business or new regions, provide customers with "touchless" claims experiences by taking advantage of new technologies such as artificial intelligence (AI), become more operationally efficient in general, or something else. Your business stakeholders have seen some product demos and are highly excited about vendor X, Y, or Z's policy administration system, claims system, or perhaps a suite of products.

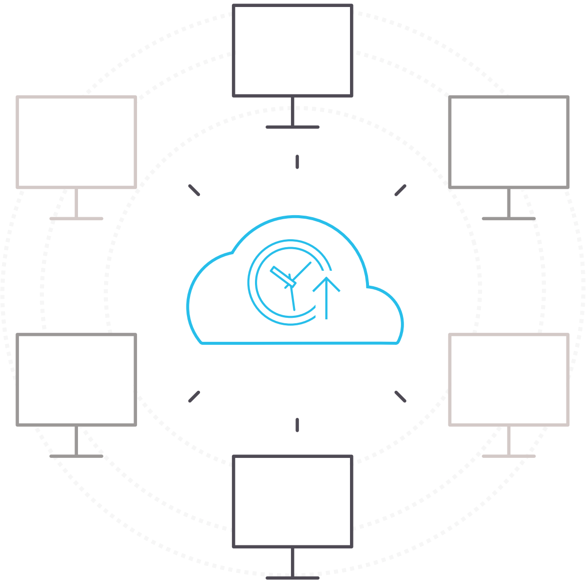
As an insurance carrier CIO or other IT leader, you've had some conversations with one or more vendors about their SaaS offerings and how they deliver their products to carriers, and now you are in a position to assess: which of these SaaS offerings will best support my organization's strategy, not dictate it? Is vendor X, Y, or Z going to give our organization the speed and agility we need to move quickly to take advantage of opportunities and pivot at a moment's notice and free up IT resources to support innovation?

As your colleagues are evaluating the products from a business use case specifications standpoint, it's time for you to dig deeper and conduct some due diligence on the short list of vendors you've whittled it down to in terms of the services, support, and computing resources provided in their SaaS offerings. From there, you'll come together with your peers and make the final decision (or present your recommendation to your board of directors) on what the best overall offering is for your organization is.

Whether it's a less formal Request for Information (RFI), your own standardized Request for Proposal (RFP) that you run, or if you are simply having a deeper dive conversation with a vendor, here are seven questions every CIO should ask - and what you should look for in responses - when evaluating the efficacy of SaaS core systems as part of your purchasing decision.

Question 1:

What results have you achieved for application availability over the past few years?



It's one thing to ask for vendor commitments to application availability (i.e. production uptime of your core systems), recovery time objective (RTO, i.e. time to recover during a disaster), and recovery point objective (RPO, i.e. the maximum amount of time that data could be lost during a disaster). It's another thing to ensure that the vendor has a proven, consistent track record of meeting and exceeding those commitments. Any viable vendor should be willing to share these actual production metrics for the past three to five years. It is also important to ensure that each vendor provides application availability metrics, not just infrastructure availability.

Also, with respect to disaster recovery, beware of vendors that by default host your production and disaster recovery instances in the same geographic region and make you pay an additional fee should you wish to have your disaster recovery instance located in a separate geographically diverse location.

In summary, when it comes to high availability and resiliency, don't just compare commitments to application availability among vendors; compare the historical results achieved, and ensure that having a robust backup location won't cost you extra.

Question 2:

How quickly can I go from signing a contract to going live in production?

In today's day and age, 3-6 months go-lives are possible, and you should ask vendors to describe recent case studies of carriers that went live in a timeframe similar to what your organization is looking to achieve. Now, getting to go-live depends on several factors, and there are exceptions to that range, so it is important to keep that in mind as you review example case studies.

Keep in mind that among line of business kits, pre-baked workflows, and third-party integration accelerators, you'll never be starting from scratch. That being said, due to the complexity of insurance and the need for carriers to modify core systems to support their visions for differentiation, there will almost always be some amount of configuration work needed. Your teams will have to weigh the tradeoff of configuration vs. going out-of-the-box.

Yet technological advances in automation are shrinking the timelines it takes for SaaS vendors to stand up hardened and implemented environments. And, of course, the relationship between you, your core systems vendor, and your systems integrator is critical to achieving faster implementations and reducing risk. Forward-thinking delivery models, staffing a mix of the vendor's own employees on systems integrator project teams combined with delivery assurance reviews, can help keep implementation projects on track and on budget, and avoid future technical debt accumulation.

Speed to market is also a function of your organization's own unique situation. Are you migrating your own mainframe legacy systems or on-premises systems (now effectively legacy) to SaaS? Or are you a greenfield initiative, launching a new business that can operate with high autonomy within its parent company? A greenfield approach certainly has the advantage of not needing to migrate existing assets, although a greenfield doesn't necessarily always guarantee speed: for example, if you're looking to launch a new insurance program in multiple states at once, you'll likely need to factor in more time for obtaining regulatory approval. Between that and other factors in creating a startup within a larger organization, it wouldn't be out of the question for greenfield initiatives to take up to a year to go live.

Getting to market fast isn't the be all end all, however. It's more important than ever before for carriers to be agile and take a test and learn approach to see what customers respond to, rather than gearing up to launch everything at once. This leads us to our next question, which is perhaps is even more important than this one.

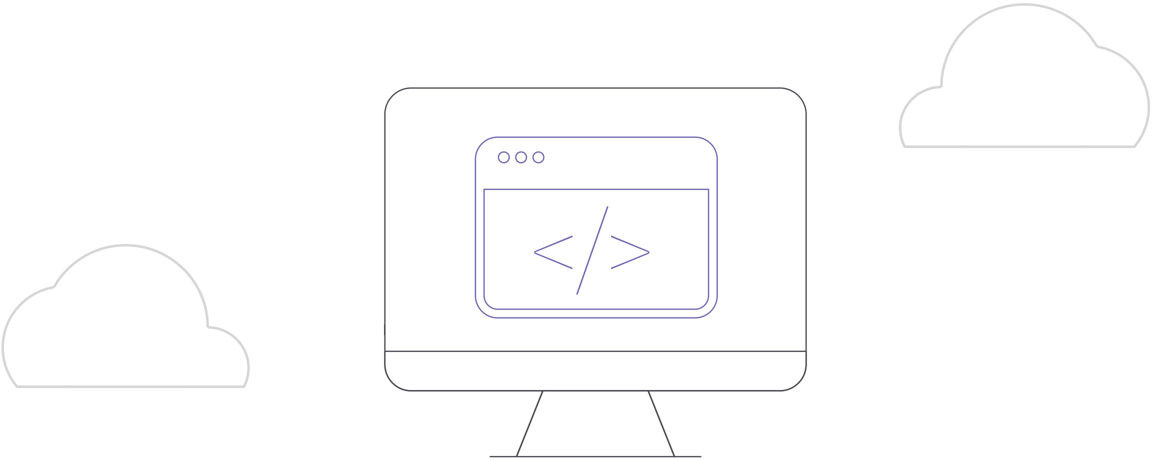
Question 3:

How quickly can I configure my core systems?

Once you've gone live with your core systems, this question really gets at "how nimble and fast will I really be?" The answer to this question can vary depending on the context within different insurance use cases, but for something such as being able to make new insurance product changes, the vendor should be able to support them as quickly as you can configure them. If a carrier wishes to make rate changes every few hours, the vendor should be able to support that – it should not take weeks or months. And as part of a SaaS license, you also should be entitled to make as many configuration updates to your core systems as needed.

Also, look for vendors that provide low-code configuration tools, which can enable business users, not just IT, to make changes quickly and easily. Of course, having a business user making a change is one thing, but getting it into production is another story. You should request the vendor to provide you with recommended DevOps processes, so that you can be confident that business and IT can collaborate in a way that maximizes all users' productivity and shortens development cycles.

In summary, look for vendors that can support your making iterative tweaks as you test and learn from what resonates with the market—whether it be to your products, policyholder or agent experiences, internal carrier workflows, or UI changes—easily and often, and for those that have strong recommended DevOps processes for moving code from your development environments into production.



Question 4:

What is your approach to security, compliance, and privacy?

This topic could be an entire eBook on its own, but let's examine a few things you should look for from a vendor in their RFP response. When it comes to security, your SaaS core systems vendor should talk about taking a multi-layered approach. No single control can be 100% effective, but by layering controls you can achieve a high level of security. Identity management, network security, vulnerability management, secure code development, regular system penetration testing, and internal threat protection measures are just some of the areas that a vendor should be heavily invested in.

Data center physical security is also important, and your vendor having a strong partnership with a major cloud provider enables them to provide carriers with some of the best physical security available. But beyond these basics, a good security program must also be designed to anticipate threats leveraging threat intelligence, react quickly to attacks with a well-practiced incident response program and have a mindset of continuous improvement to keep up with changes to attack sources and attack vectors.

From a compliance perspective, being able to validate a service provider's security program against defined standards and regulations is essential to any evaluation process. Understanding how effective a company is in using its people, processes, and technology is important to assessing their effectiveness in protecting client data. Look for vendors that maintain a comprehensive compliance program designed to meet their clients' needs, including annual SOC 1 and SOC 2 audits, PCI-DSS compliance, and maintaining ISO 27001 certification for their SaaS offering. Maintaining a robust compliance program, including regular risk assessments, also provides evidence of a company's commitment to security.

Vendors should also closely monitor privacy requirements for the P&C insurance industry, ensuring that their solutions can meet the strict requirements of privacy regulations such as GDPR, APRA, 23 NYCRR 500, and the CCPA. This area truly highlights the shared responsibilities that must be well defined when using a SaaS provider. Distinguishing between what a data owner is responsible for and what a data processor is responsible for is an important step in building a compliance program. It should be clear to you where these responsibilities lie and how vendors' solutions can be configured to meet privacy requirements.

In summary, security and trust is a topic the vendor should be taking very seriously, and they should indicate their commitment to working hard to do the things necessary to gain and maintain that trust with their customers.

Learn about our security and compliance program by visiting the Duck Creek Security & Trust Page.

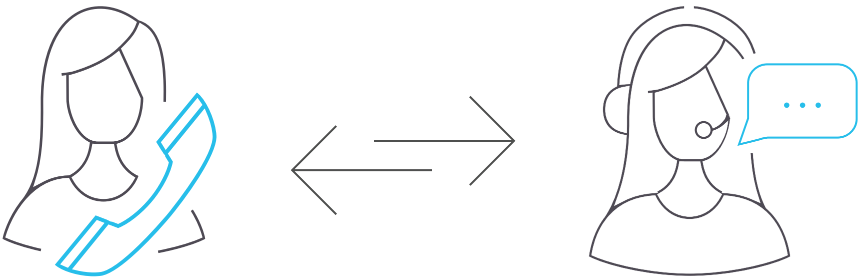
Question 5:

What's your approach to customer support?

Every vendor has a helpdesk system, but how proactive is your vendor at identifying issues and preemptively warning you in advance? In terms of customer responsiveness, a vendor should be leveraging a variety of techniques to monitor applications, infrastructure, databases, and overall security, and have robust processes in place to proactively identify and prevent incidents before they impact customers - as well as alert customers and remediate issues quickly if they do occur. There should be regular meetings with customer service managers to review application availability reports, incident tickets, and business operational goals, and the vendor should be able to speak to their processes in place for rectifying anything from a minor issue to the rare Severity 1 incident.

While many vendors may tout their commitment to customer support, look for actual signs that the vendor views support as a high priority: from making investments in a SaaS network operations center to building in-house teams comprised of both insurance industry experts and technology experts, to continuously running pilot projects such as testing out new ways of communicating with customers or further configuring monitoring tools, to collecting more relevant application telemetry data.

Finally, as situations require, a vendor should be able to operate business as usual with all personnel working remotely if needed. And in all scenarios, your vendor should provide 24 x 7 "eyes on the glass" coverage by utilizing distributed personnel spread across the globe.



Question 6:

Describe your integrations to the broader insurance vendor ecosystem. Do you provide productized integrations?

Open platforms that connect core systems to third-party data sources, analytics, and other services are critical for enabling carriers to improve their decision making across a number of use cases, from quoting, underwriting, binding, claims and more. So how should you approach assessing a vendor?

First off, not all integrations are created equal, so your decision-making criteria should hinge on much more than simply counting up how many logos a vendor has in their ecosystem. It's important to think not just about the *quantity*, but the *quality* of these integrations – not just the API calls themselves, but how those data and analytics are used in core systems workflows.

Furthermore, when it comes to SaaS, an added benefit is the ability for the core systems vendor to offer carriers *productized integrations* to today's most widely utilized P&C third-party vendors, data sources, and tools, such as motor vehicle record lookups, property replacement costs, document management systems, and more. Fully managed and maintained, these pre-built integrations ensure business continuity with full support included throughout upgrades, including fast issue remediation whenever a third-party vendor modifies their offering(s).

The takeaway: look for carriers that not only provide integrations to emerging insurtech companies, but for the data sources and tools that have already been widely adopted by the industry - they should *maintain* these for you as a service. While a SaaS vendor can't integrate with everyone, nor provide services for every third-party vendor out there, the quality of how integrations are built into workflows, as well as the services they provide, enable your IT teams to re-focus resources to develop API integrations to new third-party tools that haven't been widely adopted yet rather than spending time supporting established ones.

Question 7:

What's your approach for solving the challenges of core systems upgrades?

The industry has long known the pain of upgrades and how running core systems on-premises - or simply having your core systems hosted in the cloud - results in time-intensive and expensive upgrades that add significant technical debt accumulations. In fact, in our recent study of the European (re) insurance industry, when asked about insurance IT system upgrades in general, we found that 37% of carriers upgrade only once every 2-3 years and 16% of carriers upgrade every 3 years or more. Also, 75% of respondents reported that at some point, one of their IT systems had fallen behind with upgrades.

So what should a response from the SaaS vendor generally look like?

Ideally, the cost for all upgrades should be included in the price and handled by the SaaS vendor. You should not have to pay separately for core systems upgrades and need to hire a systems integrator each time, nor need to do it yourself as you would on-premises or if you are self-managing your core systems in the cloud. When you sign the SaaS license, it should include the application of upgrades, not just the license to the upgrades themselves, and the vendor should have robust DevOps processes in place to ensure faster upgrades, so that you no longer have to put business priorities on pause and miss out on capturing market opportunities.

Furthermore, if you are a commercial lines writer that leverages bureau circular content from ISO, NCCI, and AAIS, your vendor should have an add-on option for you to not only receive circular updates at least monthly with pre-built rates, rules, forms, UI/workflows, statistical codes, and state taxes, fees, and surcharges, but also for the vendor to maintain and apply your prior deviations and apply your new deviations for you as a service.

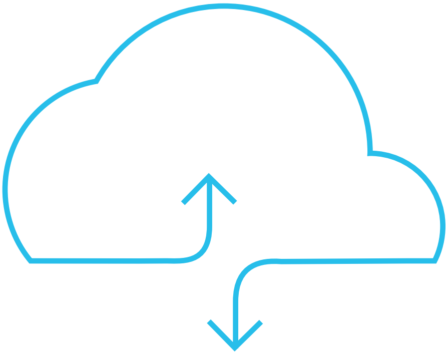
In summary, the vendor should have standardized processes in place to ensure consistent outcomes that give you the speed and agility to pursue your business strategies without fail. At the same time, the vendor shouldn't have a static approach to delivering upgrades, and should be constantly working to improve and evolve how they deliver upgrades via continuous delivery models.

Conclusion:

Bringing it all together (and bonus question #8)

From a SaaS vendor adapting new approaches to staying ahead of security threats, to describing how they monitor and communicate with customers during an incident, to conveying their approach to enabling faster upgrades, hopefully this eBook gave you a few ideas about things to ask and look for in vendor responses to your SaaS RFP or for more in-depth technical conversations. Remember, the last "S" in SaaS stands for "Service," and so as you conduct your due diligence, make sure you ask questions of your vendor and look for answers throughout the process that help you understand *"how much value am I getting not only from cloud hosting, but from the services and support you provide me?"* Beware of vendors that are solid on the former, but more ad-hoc in describing what they can do on the latter. Look for *consistency* in their approach, real measurable historical results, and a philosophy of consistent improvements to their SaaS offering so as to ensure that they not only enable faster innovation, but are also your safest choice.

To that last point, SaaS is all about continuous improvement. Vendors should not only talk the talk, but walk the walk, of showing how they are incrementally improving their SaaS capabilities - and how that evolution of their SaaS platform impacts carriers' experiences. As carriers themselves adapt to more test-and-learn methodologies to react faster to market needs, would you rather your vendor be delivering large-scale, waterfall-like changes, or proceeding with a more agile philosophy in line with your own test-and-learn approach to insurance?



Learn more about our end-to-end SaaS offering, Duck Creek OnDemand.

ABOUT DUCK CREEK

Duck Creek Technologies is a leading provider of core system solutions to the P&C and General insurance industry. By accessing Duck Creek OnDemand, the company's enterprise Software-as-a-Service solution, insurance carriers are able to navigate uncertainty and capture market opportunities faster than their competitors. Duck Creek's functionally-rich solutions are available on a standalone basis or as a full suite, and all are available via Duck Creek OnDemand. For more information, visit www.duckcreek.com.

CONTACT US

North America +1 833-798-7789

United Kingdom, Ireland, Europe,
Latin America and South Africa
+44 800 029 3523

Duck Creek
Technologies

05/2020