Jan 20, 2022

Regulatory licensing and permitting software buyer’s guide: 10 questions to ask vendors before making a decision

The world of professional licensing is only getting more complicated. Workforces in many industries are growing quickly, placing a larger burden on regulators as years pass. The health care workforce alone, for example, is expected to grow as much as 13% between 2021 and 2031. Agencies are also reckoning with an ever-changing digital landscape, one in which information must be accessed on demand and without delays. Faced with these new challenges, many regulators are turning to digital solutions to streamline permitting and licensing processes.

Real-world applications

The state of Washington recently created its own stand-alone Department of Licensing (DoL), which uses an online portal to license drivers, vehicles, and professionals. In 2021, roughly 77% of license renewals in the state were processed online.

The Vermont Office of Professional Regulation (OPR) offers another example of the power of digital government. In 2017, the state completely overhauled its licensing system, making applications for over 200 types of licenses accessible online in the process.

The transfer proved a huge success – for example, 13,000 notary public license applications could suddenly be onboarded and processed in just six weeks. Cloud-based software also opened a new range of metrics and reporting capabilities for OPR.

Exploring vendors

Choosing a software vendor can be a daunting task for government agencies of all types. In professional regulation, where the success of a particular platform can have a major impact on the well-being of the public, the stakes are higher. So how can regulators set themselves up for success when considering digital transformation?

Beyond features and functions, there are countless factors regulators must consider when vetting software vendors. What does the company’s security track record look like? What kind of support do they offer? What do other customers have to say about their solutions? Regulators must ask these and other questions throughout the process.

G2’s State of Software study from 2019 found that more than half of employees everywhere were unhappy at work because of insufficient software. By showing prudence in their vendor selection process, regulators can avoid inconveniences further down the road and better empower licensees, staff, and the public to interact with government agencies as effectively as possible.

Digital transformation requires caution
Implementing a new digital platform can also be an enormous investment in cost and time, and regulators owe it to themselves and the public to make educated, pragmatic investment decisions. Here we will break down the basic (and more complex) questions regulators should ask when choosing software vendors.

1. Is the software configurable?

Regulations everywhere are continuously evolving, and change is inevitable. Some regulators in growing industries may even require new license types as time goes on. So how can software enable us to make changes without heavily relying on IT teams?
Government agencies shouldn't have to wait months to update a title or make changes to attestations. A proper software vendor empowers agency staff members to make easy adjustments themselves, on the spot, with minimal effort.

Choosing software that can grow with your agency
Regulators must ask themselves how easily their software can be configured to fit their needs and workflows. An exemplary software vendor understands each agency has its own nuanced approach and tailors its solution to fit the regulator's needs.
Agencies should look for a solution that can grow as the agency grows. Using a system that can be adapted to meet different needs and doesn't quickly become outdated and dependent on IT is key. Ask prospective vendors how configurable their software will be when it's in your agency's hands.

2. Does the software feature role-based permissions?

Some of the information regulators have in their records is highly sensitive and should not be accessible by all staff. Regulators must often assign staff members, based on their roles, certain activities and access privileges.
Role-based permissions are useful for a couple of reasons. They keep certain users from accessing information that is unnecessary to them, but they also allow administrators to keep a bird's-eye view of the agency and its staff network.
Occupational licensing software should allow agencies to assign role-based permissions individually, to avoid revealing protected information to unauthorized users. By using vendors that offer this feature, regulators can further ensure the safety of sensitive information.

3. Does the vendor have regulatory expertise?

Though rare, software vendors with real-world regulatory experience enjoy a critical advantage when offering digital solutions to the public sector. Vendors lacking deep knowledge of regulatory processes are unable to create and configure effective solutions that align with industry best practices and varying regulatory approaches.

Does the vendor understand unique industry requirements? Can they be a partner in your success? Or do they simply offer a cookie-cutter solution? Software partners with field experience offer regulators platforms tailored for their specific needs while offering experience-driven insights along the way.

Expertise allows a vendor to return to the regulator with strategic advice that involves little handholding. An adaptable, experienced software provider can craft, for example, 75% of a solution for an agency, while a custom-built solution with little support places the burden entirely on the regulator.

A vendor should know the regulator's overarching needs and approach each meeting with specific questions and suggestions for implementation. Providers with expertise can even offer advice based on their own experiences, shortening timelines and streamlining workflows for everyone involved.

4. What reporting and analytics capabilities does the software have?

Few understand better than regulators how difficult it can be to track performance and accurately gauge success. Regardless of complexity, government leaders still must endeavor to capture relevant data as thoroughly as possible and present full performance reports to their administrative boards.

When choosing a regulatory software solution, regulators must ask: does the prospective new system allow users to leverage data to draw conclusions, drive insights, and help with strategic decision-making? Many systems allow for data input, but it can be difficult to retrieve and process this data, much less make sense of it.

Dynamic, intuitive querying

Using software, agency staff should be able to create full reports with dynamic analytics on demand. Good vendors can bring together data from different sources into a single system for more accurate reporting and a more comprehensive picture of the agency.

Does the software solution allow staff to adjust query parameters quickly and easily? Does it include dashboards for your executive directors or staff to visualize data in a way that's both comprehensive and easy to understand? Can the solution automate pulling and sending reports for regulatory filings? Can executives effectively track key performance indicators?

Creating custom reports

A robust piece of regulatory software empowers its users to create customized reports on demand. Indexing and cross-referencing pieces of data like, for example, the number of complaints submitted or the number of people in a call queue can help staff to draw specific and powerful insights on their work within their industries.

Reporting enables regulators to be more proactive in their governance. Agencies with serious reporting capabilities can better manage risk and decrease the rate of non-compliance and unlicensed activity, as they can use data to get a pulse on their industries at given any point. Comprehensive reporting and analytics capabilities are crucial to any digital licensing solution.

5. Is the interface easy to use?

A system is only good if it's used. Even the most complex and powerful software solutions can be limited if they are not user-friendly and accessible to staff. When browsing between vendors on the merits of their interfaces, agencies should consider the following:

- Compatibility – is the platform accessible through the most common devices (cell phones, desktops, tablets, etc.) by staff, licensees, and members of the public?
- Intuitiveness – does the information flow in an intuitive manner? Can staff quickly access multiple queries and arrange them in a digestible way? An intuitive interface leads to less reliance on IT support and fewer complaints from licensees and members of the public.
    - An intuitive interface allows users to adapt to the system more quickly. This leads to fewer calls from frustrated licensees. Many working in regulatory agencies have dedicated their lives to public service, and an easy user experience offers a powerful way to enrich the lives of the citizens to whom they are beholden.

  - Consistency – does the software facilitate a consistent user experience across the system? Consistency in design and function means a software platform can be adapted quickly and users can learn how to navigate for the information they need without too much external support.

Most vendors will still offer training and IT support services to make sure regulatory staff know how to use their software effectively. But by considering ease of use from the start, agencies can undergo a quick implementation process and empower employees to harness the full power of regulatory software within a reasonably short time span.

6. What is the vendor's security protocol?

When evaluating vendors, regulators must ask: what are they doing to make sure data is protected against cyberthreats? If they outsource their security systems, what protocols are *their* vendors using to safeguard information and mitigate the damage of successful breaches?

Finding a comprehensive security approach

Cybersecurity typically demands a multi-pronged approach. For example, even the most robust software solution can fall short if the vendor's staff doesn't have the expertise to implement and secure it properly. Beyond comprehensive cybersecurity training, agencies should make sure their vendors only provide staff with access to information on a need-to-know basis.

The physical security of a data storage system is fundamental to its overall integrity. Agencies should ensure their vendors use systems (proprietary or third-party) that have the physical capability to maintain 99.9% uptime and create continuous data backups. By using vendors who are compliant with ISO/IEC 27001/27017/27018/27701, SOC 1/2/3, PCI DSS, and other physical security protocols, agencies can ensure thorough protection of sensitive information.

To guarantee the highest level of cybersecurity compliance, a vendor should also implement multiple application security measures, including routine source code review, static application security testing, dynamic application security testing, and much more. They should have a robust network security infrastructure that uses practices like network segregation, web application firewalls, and intrusion detection/prevention. Be sure to ask if a vendor's systems are routinely updated and patched in response to new developments in cybercrime.

The costs of poor cybersecurity

In the event of a cybersecurity incident, a regulator left scrambling without backups, or a disaster recovery plan will likely face a longer period of system interruption. Fixes may require time and resources, especially if they involve potentially compromised data.

Data breaches also present direct financial consequences, particularly when regulators choose to pay the cybercriminals involved. When attacks do not involve data held for ransom, there may be other costs associated with actual or potential breaches, including:

- Payment of insurance premiums.
- Legal and administrative costs.
- Investigation and consultancy costs.
- Labor costs, such as overtime pay for staff to deal with the attack.

Cyberattacks cost more than just time and money, too. They can erode public confidence in a regulator's ability to keep sensitive information safe. When choosing between software vendors, security must remain among an agency's foremost priorities.

7. Does the software offer self-service functionality?

How can a software solution reduce the burden of labor on regulatory staff? Does the platform have self-service functionality so that users are able to digitally access pocket cards, quickly update their personal information, or provide information to request the regulator to update their records?

With a proper regulatory software solution, users should be able to set in motion processes like updating tombstone data, updating CE credits, accessing invoices, and making payments all without staff intervention. This reduces call volumes and means licensees can serve themselves, from wherever they want, 24 hours a day. They don't have to wait for operating hours.

8. Can processes be automated?

Automation can significantly reduce staff touchpoints and free up employees to handle tasks that require actual human judgement. For example, an automated online license application form can cut paper out of the process entirely, removing the burden of scanning hard-copy applications and inputting their data into a system.

A proper software vendor should have automations in its system that help accelerate the licensing and permitting processes and allow staff to redirect their efforts to other strategic initiatives. How exactly does the software help reduce staff workload? Regulators should ask the following:

- From initial application to document upload, payment, applicant notification, and beyond, can the licensing or renewal process be completely automated?
- Are there automated workflows for staff to quickly process and verify licensee information, so that all tasks can be performed in a timely manner?
- How does the solution automate routine tasks like ensuring reports are submitted on time?

Automations are a critical part of the software package offered by any given vendor. They save regulators countless resources in the long run and can be implemented with relative ease and efficiency. Any reputable vendor should have at least a basic arsenal of software automations at its disposal.

9. Does the software offer APIs and integrations?

Many regulators find themselves burdened with multiple discrete, siloed databases containing information formatted in different ways. This can make the work of pulling and compiling information from these sources unnecessarily tedious and time-consuming. But, if agencies choose vendors that use APIs and software integrations, they can easily consolidate their data and create a single source of truth from which to draw insights. A software solution that fully utilizes the power of integration can:

- Communicate with key third-party applications to create a connected agency and a holistic view of licensees.
- Facilitate seamless interagency, interdepartmental, and interstate data sharing.
- Save time normally wasted manually entering data into multiple systems.
- Empower agencies to create more end-to-end workflows and processes.
    - For example, by having an education provider integrated, an agency can more easily retrieve test scores, licensees can be booked faster for exams, can select courses they completed etc.

Some of the most fundamental must-have integrations for regulators include integrations with exam platforms, educational institutions, workforce databases, and national/state repositories. By configuring a software platform to pull and utilize data from legacy systems and other siloed databases, regulators can make communication easier and more effective across the board.

10. **Does the software provide a 360-degree view of the regulatory entity?**

    To effectively track their own progress and adjust their priorities, regulators must have a comprehensive picture of the entities they are overseeing. Will the potential software solution provide staff with a full view of all the license applications in its system? Can staff navigate the connections between different pieces of information all within one easy-to-use dashboard?
    Will the software give you an audit trail of every action taken by a person, entity, or business, both before and after the application process? Good regulatory software provides a complete view of the licensee or business, including details like employment history, educational history, continuing education, payments processed, and much more.

Digital transformation is an undertaking that should be approached with extensive planning and attention to detail. Government agencies must make sure new software solutions are secure, robust, and easy to use *before* expending the resources necessary to implement a new system. Their platforms should be intuitive and accessible from any user end point, through any commonly used device.