

WHITEPAPER

Top 5 Considerations for Modernizing Technology Platforms in State Regulatory Agencies

How a modern SaaS cloud architecture solves obstacles in transforming the regulatory environment



A man in a suit and glasses stands on the right, gesturing as if presenting. Three people are seated at a table in front of him, listening. The scene is set in a modern meeting room with large windows and indoor plants. The entire image has a red color overlay.

Deciding how to modernize the hundreds or even thousands of applications being used by multiple agencies across a state, or by multiple boards under an agency, is no simple task.

Summary

This whitepaper discusses the top considerations for modernizing technology platforms in state regulatory agencies. It emphasizes the importance of robust security, data consolidation, alignment with standards, solution selection and implementation, and seamless integration.

By leveraging technology with a modern SaaS cloud architecture, state IT departments and CIOs can help regulatory agencies address these considerations and implement a customized platform with improved security, efficient data management, self-service capabilities, and reduced operational costs. This paper also highlights the challenges faced by state agencies in terms of security risks, data consolidation, adherence to standards, platform selection, transitioning from legacy systems, and provides actionable steps and recommendations for achieving successful platform modernization in regulatory agencies.

Unique regulatory challenges, unique technology requirements

When it comes to regulatory licensing across state-level governments and regulatory agencies, the indispensable contributions of state information technology departments and CIOs cannot be overstated.

Together, state IT departments and CIOs support regulatory agencies in numerous ways by:

- **Acting as strategic partners to regulatory agencies**, enabling them to leverage technology effectively to achieve their goals, enhance operational efficiency, ensure compliance, and deliver better services to citizens and businesses.
- **Working closely with regulators to develop strategic plans** that align technology initiatives with an agency's objectives, ensuring that investments support the agency and state's mission.
- **Providing the necessary IT infrastructure to support the operations of regulatory agencies** – from network infrastructure, servers, databases, and software applications, to cybersecurity, data storage, etc.
- **Managing the software implementation process**, which includes gathering requirements, selecting the appropriate solution, running a risk assessment, overseeing configuration, and executing a smooth deployment.

State IT departments and the teams working directly with these regulatory agencies seek to find platforms that meet the specific needs of those agencies while aligning with broader statewide IT objectives. Examples of these common objectives include reducing data center footprints, improving security, or rationalizing the number of applications within their state IT portfolios.

Deciding how to modernize the hundreds or even thousands of applications being used by multiple agencies across a state, or by multiple boards under an agency, is no simple task. States must rationalize the technology they are using as well as the people, processes, data centers, and other components of their technology programs.

In this paper, we will look at **five of the top challenges facing state IT departments** as they collaborate with regulatory departments, agencies, or divisions to modernize their licensing management platforms.

1

Maintaining security in an ever-evolving technology landscape

US pipeline cyberattack is a 'wake up call' for America

By Matt Egan, CNN Business
Updated 2:49 PM ET, Mon May 10, 2021

Regulator Proposes \$1 Million Fine for Colonial Pipeline One Year After Cyberattack

By Edward Koppenhaver, CNN
Share American Dental Association hit by new Black Basta ransomware

Ontario nurses' regulatory body investigating 'cybersecurity incident'

The College of Nurses of Ontario regulates about 195,000 nurses in the province

By Lawrence
Kate Dubinski · CBC News ·
Posted: Sep 17, 2020 11:07 AM ET | Last Updated: September 17, 2020



At a time when state systems are increasingly being breached and ransomware attacks are commonplace, security is the top requirement for any new platform being adopted. Further complicating matters is the fact that the risk environment is dynamic and ever evolving. State government entities and regulatory agencies must adapt in real time to detect and neutralize new threats. Yet all too often, hackers successfully gain access to sensitive citizen data and disrupt important government services.

For example, the Washington State Department of Licensing (DOL) suspended their Professional Online Licensing and Regulatory Information System in January of 2022 because of a suspected data leak. The incident targeted professional and occupational license data specifically, including personal information like social security numbers.*

One of the primary difficulties arising from the utilization of long-standing, inadequately maintained platforms is the inherent security risk they pose. As hackers and other threat actors develop new techniques, legacy systems become easy targets. For example, in some cases, agencies continue to use old infrastructure that no longer has support from the vendor. This means, if something goes wrong and the system stops working or data is lost, there is no customer support from the vendor – a disaster waiting to happen.

*Wilkinson, Eric. (2023). Washington Department of Licensing experiencing system disruption due to a cybersecurity incident. KING 5 News. Retrieved from <https://www.king5.com/article/news/local/washington-department-of-licensing-hack/281-79a653bd-25b9-4fd8-899c-ec900e1b8d2c>

Cloud-based licensing platforms for security-minded states

Security advantages of a modern cloud-based platform include:

- **Cloud-based platforms offer comprehensive solutions managed within a secure cloud hosting environment**, ensuring that data and customized support remain within the sovereign jurisdiction of their customers, providing enhanced security for security-minded states.
- **Leading cloud platforms provide regulatory agencies and government specific security features, controls, and certifications** as part of their core platform services.
- **Using a cloud-based platform effectively means outsourcing security features to the cloud**, which may result in better overall security than the state can provide on its own.
- **Having a single solution means all data stays in one place**, further reducing security risk.

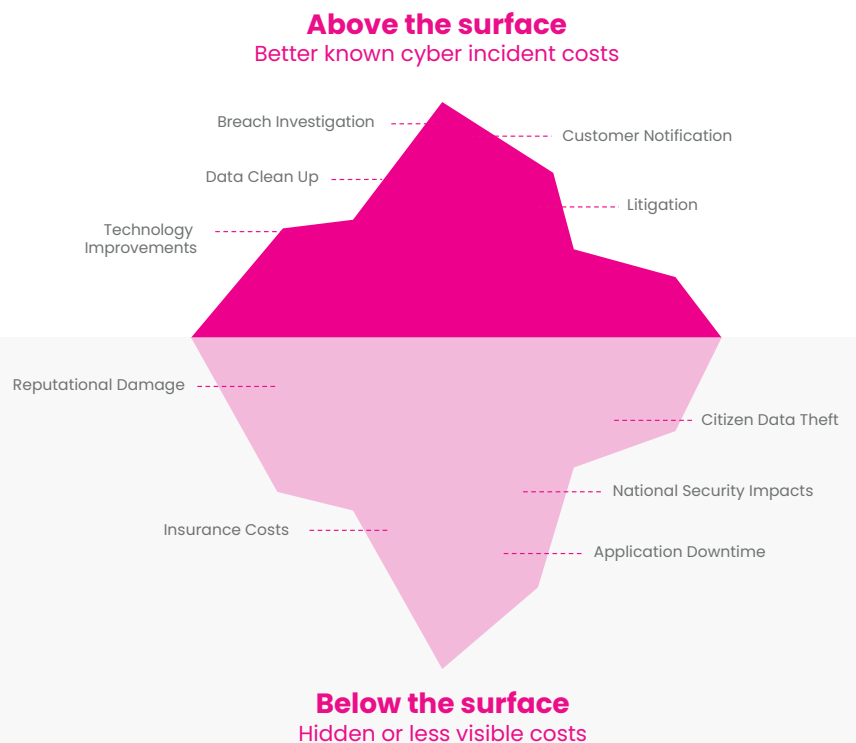
Evaluating security for a regulatory information system

When evaluating security for a regulatory information system, it is important to:

- **Review the entire solution from end to end**, including any custom-built components, extensions, integrations, and operating models to ensure they provide proper security controls.
- **Ensure it is designed as a solution that meets the specific requirements** for state government and regulatory agencies.
- **Review all code thoroughly**, as some systems can require a significant amount of custom code that is built on top of generic platforms. If that code has security flaws or can be exploited, it becomes a risk.

In addition, if the overall platform does not come with an operating model that actively monitors and responds to security alerts and incidents, then security flaws can be exploited without notice and cause long-term, sometimes irreparable damage.

The hefty cost of cyberattacks on government



Bringing data together from disparate sources to drive greater intelligence

Data represents a unique opportunity to generate insights, improve productivity, and deliver more personalized customer service. However, states face a significant data challenge across different siloed applications and agencies. State CIOs and agencies are left to determine how to reduce the number of data silos, consolidate information into one place, and use it to provide valuable insights that can inform decision making.

Within a regulatory agency, data availability offers a valuable opportunity to effectively identify license applications or renewals that carry a higher risk and respond appropriately by flagging them accordingly. For example, licensees in many states are not allowed to obtain or renew their license if they have not paid their taxes or child support. But in many states, the data about tax payments, child support payments, and licensing are all in different databases and systems, making it difficult to know if a particular applicant is ineligible for a license. States should look for solutions that are able to bring all this data together, making it possible to flag if individual applicants are not in good standing. Having a holistic view of data can provide many valuable insights, such as where there are potential risks (as in the example above), as well as how productive the state's workforce is and whether it is meeting its goals.

Exploring AI applications in state data management

An emerging solution in this realm involves leveraging artificial intelligence (AI) to handle state data management. AI tools are currently being developed across various sectors, offering valuable assistance to state departments.

Consider the following potential avenues for implementing AI within state departments and regulatory bodies:

- **Natural Language Processing (NLP)** – NLP tools are used to enable analysis and understanding of human language. For regulatory bodies, NLP can be used to review applications or implement a chatbot for constituent communication.
- **Predictive Analytics Platforms** – These tools use algorithms to analyze data and predict outcomes. Regulatory bodies can use these tools to forecast licensing demand or optimize resource allocation.
- **Compliance Monitoring** – Some AI-based solutions can help with compliance monitoring by analyzing large volumes of data in real time or identifying non-compliant activities efficiently.

One function that would benefit from the use of AI is profiling for risk of applicants and licensees. Regulatory agencies are mandated to protect the public by identifying licensees that pose a risk to their safety, are violating ethical guidelines, or are fraudulent.



How to ensure your regulatory software aligns with state and industry standards:

- Choose software that has obtained security certifications such as PCI, SOC, and ISO 27001.
- Choose software that is partnered with a secure cloud hosting environment, like Google Cloud.
- Ensure the software mandates have ongoing security management built into the license agreement.
- Ensure the software includes continual upgrades to meet the latest security threats.

State IT departments are actively working towards implementing integrated platforms for various functions, aiming to break down silos and foster collaboration across divisions, departments, and agencies. They may establish platform standards for key capabilities and services such as business intelligence, cloud platforms, security tools, monitoring, or customer experience management. Depending on whether regulatory agencies are centralized or decentralized, there may be several license management platforms or other solutions deployed across different agencies.

In reviewing the requirements for regulatory agencies, it may be tempting to try and align these needs with more broad generic customer experience, business process, or case management requirements and to select generic platforms such as CRM platforms, web content management, or database platforms as common standards. However, in our experience, regulatory agencies have specific functional requirements that tend to stretch the capabilities of these generic platforms to the point where significant customization is required. In making the tradeoff between adopting a generic platform versus selecting a platform specific to license management, the amount of customization required to meet these needs should not be underestimated.

In addition, while there can be some common processes and services across regulatory agencies, supporting configuration of these platforms to meet the unique requirements of each regulatory agency, without needing significant custom development, becomes key to success. Licensing management systems need to provide sufficient "out-of-the-box" workflows, features, and portals to provide common services to these regulatory agencies while still allowing for rapid configuration to support requirements specific to each agency.

3

Choosing the right solution and ensuring a smooth transition

Numerous agencies continue to depend on outdated legacy solutions to handle their regulatory licensing and permitting processes. These solutions encompass a range of antiquated methods such as paper-based workflows, manual processes, fragmented systems like Access databases and Excel spreadsheets, all of which were conceived long before the advent of cloud computing and mobile technology. Unfortunately, these outdated solutions give rise to perpetual frustration among staff members. Not only do they demand countless hours of manual data entry, hindering the efficient retrieval of relevant information for reporting and auditing, but they also lack the capability to securely access data from any location or device.

While the need to move away from these legacy solutions is clear, the challenges states will encounter doing so are two-fold. First, they must select the right platform to meet their requirements. Here, states often get caught up trying to build their own regulatory information platform on generic CRM platforms. The problem with that approach is that these generic platforms are not purpose-built to manage the data, workflows, portals, security, and business rules specific to licensing or permitting regulation.

Selecting a platform specifically designed for regulatory agencies

While the initial affordability of a generic platform may seem appealing, the overall cost of ownership becomes substantial due to the frequent requirement for consulting services to implement and customize the platform, ensuring it aligns with essential regulatory requirements. Selecting a platform specifically designed for regulatory agencies is critical to saving time and money.

Red flags to look out for when evaluating a generic platform for regulatory use:

- It is not designed to be used "as is" to perform regulatory functions**

Generic platforms require multiple third parties, custom code, acquisitions and/or other independent software vendors to carry out capabilities like license renewal, full auditing of complaints management and case management, continuing education management, etc.
- It presents security threats**

Since generic platforms cannot perform regulatory functions without third-party software, using them compromises the integrity of the environment. Third-party software means a more complex technical environment, opening your agency up to cybersecurity threats.
- It does not provide backend payment processing**

With generic platforms, most agencies are not offered low-cost alternatives for payments or shown a way to reduce the burden on IT without costly backend payment providers.
- It presents compliance and regulation complexities**

Government regulators operate within a complex landscape of compliance standards, laws, and regulations. Generic platforms likely don't adhere to these specific requirements and often need significant customization.
- It is not made to withstand the evolving regulatory landscape**

Regulatory agencies and compliance standards are subject to frequent changes and updates. Generic platforms struggle to keep pace with these requirements since they are not flexible and are made for broad application. This often leaves agencies in a constant cycle of customization, leading to delays in implementing new regulations.



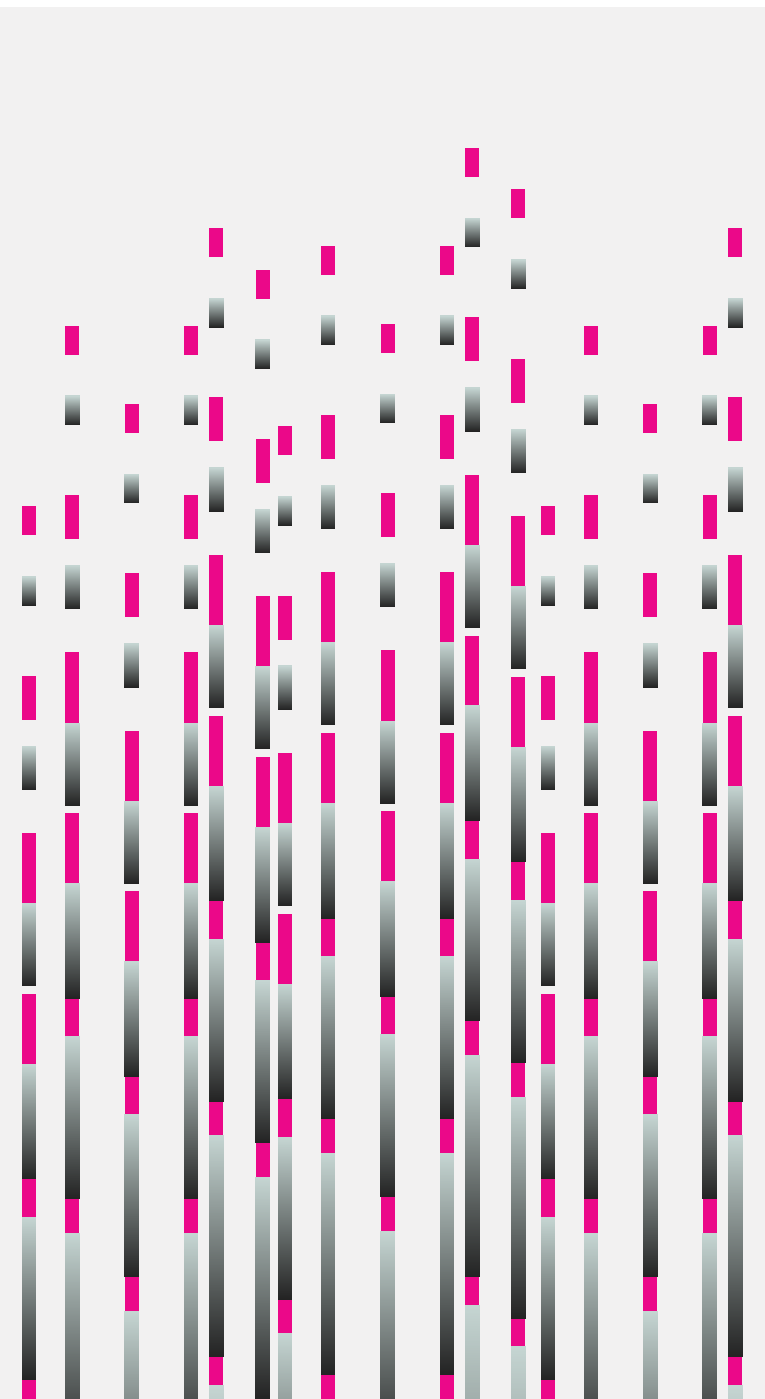
In summary, the use of purpose-built platforms designed specifically for regulatory agencies is crucial, as they offer tailored functionalities, ensure compliance with regulations, provide secure data access, and minimize the need for costly customization. Choosing a purpose-built platform addresses these above issues, enabling agencies to overcome the limitations of legacy systems and achieve streamlined operations in a rapidly changing regulatory environment.

Migration challenges, clean-up, data transfer, retraining, and more

The second challenge is that there will always be some demanding work in migrating to a new system, as it requires cleanup, data migration, retraining the workforce, and other complex tasks to successfully transition from a legacy system to a cloud-based one. It is a substantial undertaking for any agency, but the benefits of doing so include greater productivity, better customer support, higher data quality, and lower operational costs – to name just a few.

Actionable steps in managing migration to a new platform:

- **Evaluate your current system**
Conduct process mapping to understand how current regulatory processes are performed (note resources and time required).
- **Define a migration strategy**
Clarify what goals, timelines and resources are realistic for your organization (note your budget and government legislation).
- **Prioritize data clean-up**
Ensure staff is allocated to remove redundant or incorrect information and develop an approach to move any paper-based information into a cloud based-system.
- **Leverage your vendor's expertise**
Keep open communication with your vendor, take advantage of any training materials they provide and develop a relationship with their customer success team.
- **Train your workforce in the new system**
Ensure proper training for staff and develop communication and change management plans. This may require extra support so getting a head start is beneficial.
- **Test before full implementation**
Test the system on a small group of applicants or licensees, and staff members. Troubleshoot and identify pain points that need solving before rolling it out agency wide.
- **Engage in continuous monitoring**
Once implemented, track key metrics, and collect user feedback. The system will need updating as new regulatory requirements and technological advancements emerge.



Striving for seamless integration, future extensibility, citizen self-service, and low code configurability



90x

acceleration in the speed-to-approval for new licenses



100%

license applications submitted online

In Nevada, the Chiropractic Physicians' Board implemented a cloud-based solution and moved 100% of license applications online, which resulted in a 90X acceleration in the speed-to-approval for new license applications. The new system offered digital-first, self-service capabilities which has greatly simplified the application process for applicants and licensees. This self-service functionality has reduced regulatory staff intervention.

When states assess new technology options, a critical factor they consider is the ability to seamlessly integrate the solutions with their existing technological infrastructure, encompassing data warehouses, identity management solutions, and various other platforms. A straightforward illustration of this is the objective of enabling employees and citizens to access the technology using a single set of state-wide login credentials that provide universal functionality across all platforms, eliminating the need for separate logins to each individual solution. If modern technology does not integrate seamlessly with existing platforms, it may very well not be the right choice. Additionally, it is important to consider platform extensibility to ensure that the technology infrastructure can scale and expand as state government and agency needs evolve, or as new requirements arise.

Another essential aspect to consider is the inclusion of self-service functionality for citizens. Presently, numerous regulatory bodies lack self-service capabilities within their application systems, which means that applicants and licensees using these systems are unable to autonomously manage their documentation or information. Consequently, regulatory staff are burdened with additional responsibilities, including the laborious task of gathering information, accessing documentation on an ad hoc basis, and consistently following up with licensees, leading to increased workload and inefficiencies. When equipped with self-service functionality, applicants and licensees are empowered to complete tasks independently and on their own time.

After acquiring and configuring a platform, states also seek the ability to independently make modifications without being reliant on vendor assistance. In the context of a licensing management platform, that might include being able to add a new rule, setting the parameters for a new fee, or creating a new customized report. Being able to make these kinds of changes independently is critical to being agile and ensuring that the solution is always precisely configured to meet the state's unique needs. To achieve that, states would be wise to select platforms that are not custom built, opting instead for solutions that are low code and highly configurable.

The future of regulatory transformation

In 2023, the Center for Digital Government (CDG) released a survey revealing that state and local governments are investing in modern technology more than ever. Of the governments surveyed, **56% said they will be upgrading technology solutions by 2025**, citing operational efficiency as a top driver.* In addition, CDG's surveys of state, city, and county governments reveal that newer cloud-based technologies deliver better experiences that meet constituents' modern demands.

State IT departments and central regulatory agencies across the U.S. are undeniably confronted with a formidable challenge of modernizing regulatory environments. The tasks at hand seem endless, encompassing various aspects such as selecting the appropriate software platform, ensuring its compliance with standards, facilitating seamless integration, and providing workforce retraining to adapt to the new system. Embracing modern SaaS solutions enables state IT departments to transform the regulatory environment, delivering efficient and secure services to constituents.

To stay up to date with digitization of paper-based systems, selecting a configurable solution empowers states to make changes independently, promoting agility and customization to meet specific regulatory needs.



56%

56% of state and local governments will be upgrading technology solutions by 2025



To stay up to date with digitization of paper-based systems, selecting a configurable solution empowers states to make changes independently, promoting agility and customization to meet specific regulatory needs.



Thentia is already creating huge efficiencies for regulators across the globe.



Oregon State Board of Licensed Social Workers



Nevada State Board of Medical Examiners

Let us show you how Thentia Cloud is partnering with state agencies just like yours.

Join the ranks of forward-thinking state regulatory agencies that have harnessed the transformative potential of Thentia Cloud.

+1 800-961-1549 sales@thentia.com www.thentia.com



SCAN TO BOOK A DEMO