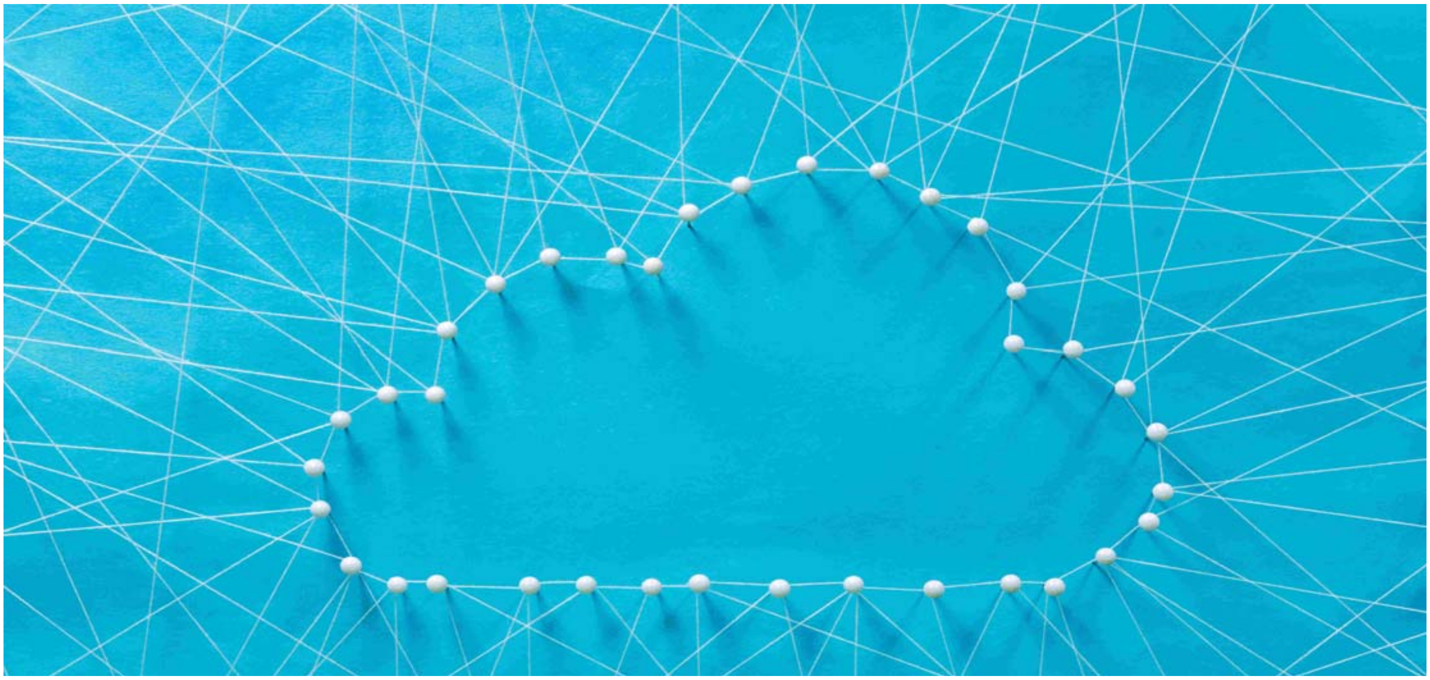


Why the new federal shared services vision isn't the same old SaaS

The US federal government has been on the shared services journey for quite some time. The concept of agencies sharing infrastructure, software, and people to perform common government functions makes sense. If executed properly, shared services can allow agencies to better focus on their mission, achieve cost savings from fewer duplicated functions across the government, and improve standardization and internal controls. One area that has been a particular focus for government sharing has been administrative systems (e.g., HR, Finance, and Acquisition). Does it really make sense for each agency to implement and operate its own administrative systems?

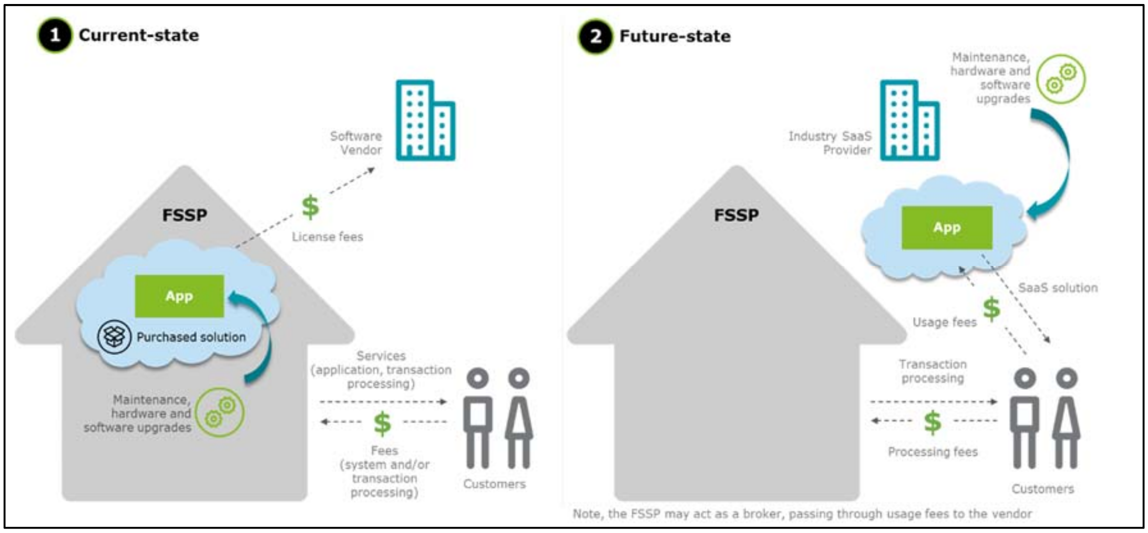
As the government has made progress on having agencies share other agencies' administrative support systems, a major issue has challenged its progress – funding for providers' investment in solutions and capacity.

Unified Shared Services Management (USSM) recently released a new vision for federal shared services to address this challenge by reducing upfront investment in systems. In this vision, the government purchases Software as a Service (SaaS) solutions for administrative functions. Many of you may be wondering "Doesn't the government do this already?," or "My solution is already hosted in the cloud," or "I'm using a Federal Shared Service Provider (FSSP) and not hosting the solution, isn't that Software as a Service?"

This paper attempts to demystify the new vision and discuss how, once realized, it can benefit the federal government. The two primary differences between USSM's vision and the existing federal shared services environment are 1) How the solution is priced and 2) How the solution is delivered.

How is the solution priced?

The new vision is to obtain solutions from industry using a SaaS model, which is billed as a utility rather than using government-owned software, purchased by the FSSP. Note that the customers may go directly to the SaaS provider or go through an FSSP that has a relationship with the SaaS provider.



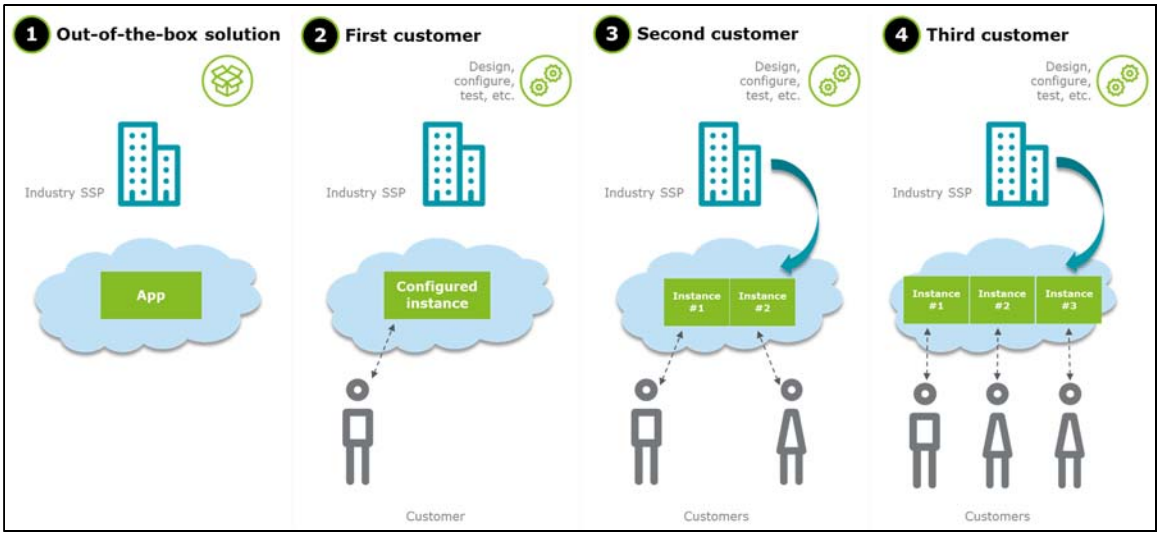
Current-State: Today, FSSPs generally buy an application from the vendor and host it themselves. They may contract with industry for infrastructure/hosting and application maintenance, but the FSSP is responsible for the cost of licenses, maintenance, application management, configuration, and upgrades (both hardware and software), which they pass on to the customers. This model creates challenges for the government because FSSPs can retain only a small percentage of the fees they receive from customers. Therefore, when an FSSP modernizes its solution to accommodate new regulations or new releases, it must pass these costs through to customers when they are incurred. This can result in customers having to pay for large upfront costs or spikes in bills that they often cannot afford or accurately forecast. If the government remains on the current path for shared services, agencies will consolidate on a smaller number of modern systems, but 5-10 years from now, these systems will be legacy systems and there will likely be a spike in cost to update them.

Future State: In the SaaS model envisioned by USSM, the application is hosted by the software vendor in the cloud and billed as a utility either directly to customers or to the FSSP (which passes on these usage costs to the customers). While some FSSPs and agencies have their applications hosted in the cloud today, they are still paying for licenses instead of usage. This means they might still have funding challenges when it is time to upgrade their solutions. In the future state pay-as-you-go model, customers will have access to the latest hardware and software upgrades (and will not be billed directly for it as they currently are). It is like when your SaaS email provider patches their software or upgrades their infrastructure using the latest hardware; they just do it – they do not send you the bill.

How is the solution delivered?

The new federal shared services vision is not to just move everyone to the cloud (which merely changes the infrastructure and charge back model). The vision is that the government moves to standardized SaaS solutions that require minimal customization and enable costs to be shared across multiple customers.

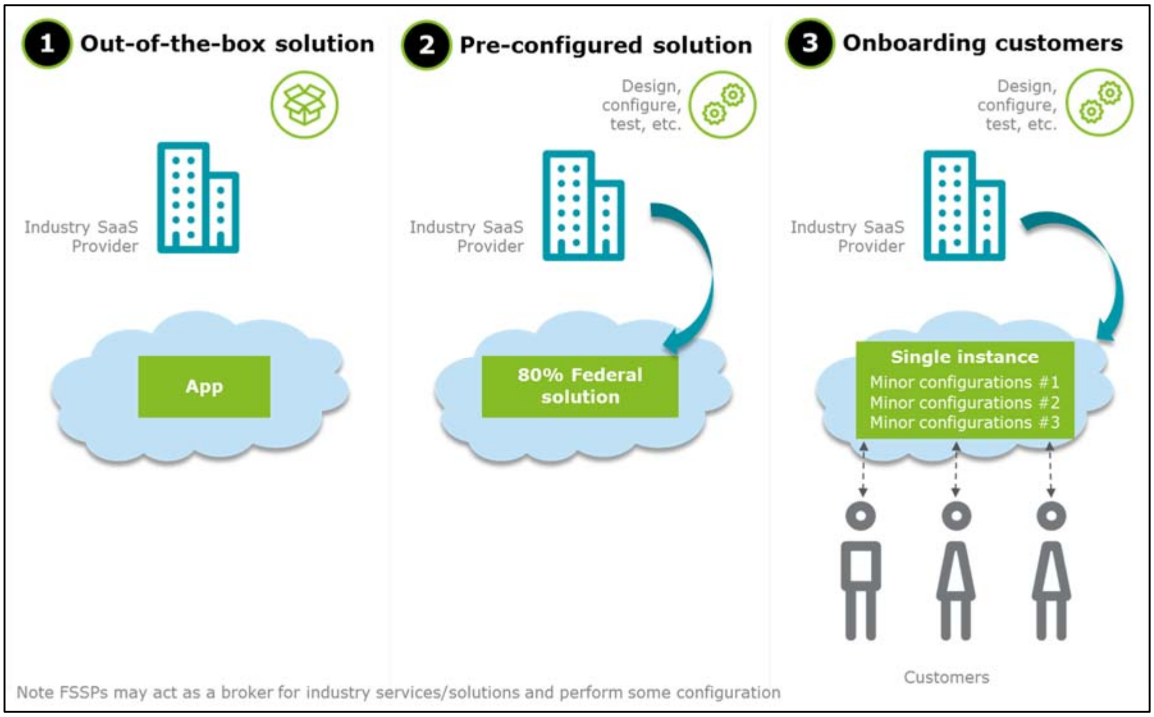
Current State (Multiple Instances)



Some FSSPs are currently using applications that are hosted in the cloud. In this example, they typically move several agencies into a single instance. However, agencies that have partnered directly with industry to have their administrative applications hosted in the cloud are not sharing a single instance. In the current model, each time a new agency migrates to the cloud application, the vendor configures an instance of the software to meet the customer's requirements and goes through the usual process to design, configure, and test the solution. This happens over and over again, with the vendor stacking up instances of the same application that all have to be individually maintained. Therefore, when it is time to make a change to the software to accommodate a new regulation, this change has to be made in each instance (and tested and deployed) and each customer has to pay for these changes. Even if the vendors started charging by usage, the charges would still be high because they have to make updates and maintain each of these individual instances.

Moreover, since the customers are all federal entities, the likelihood is that about 80% of their requirements and workflows are the same – so why go to the trouble of maintaining separate instances? Why not move towards a single instance? Spoiler alert: you can. The biggest resistance to this used to be data security, but that "issue" is now a red herring. The technology is mature enough to not need separate instances to deliver data security, which leads us to the future state. In fact, a single instance is likely more secure.

Future-State (Single Instance)



In the future model, the federal government standardizes its business needs, data structures and performance standards, allowing vendors to pre-configure a solution to meet the "80% requirements." Think of it like this: all federal entities pay bills. The process to pay a bill is (or should be) pretty standard. When onboarding customers to the new solution, the SaaS provider may still need to make small configurations and customizations based on each customer's unique requirements –stemming from their unique mission or regulatory environment. However, the vendor saves the cost of building and configuring a new instance each time a new customer comes onboard and the cost of maintaining multiple instances. These costs savings can be passed along to customers in the form of lower usage fees.

The one caveat to the single instance is there may be certain groups of customers that have a business that's significantly different than other entities and therefore impossible to use the same configuration/workflow. In this case, a separate instance could be used for that customer and others that are similar (e.g., an instance for loan/grant making agencies). Even with this exception, there are significant economies of scale versus the current state.

Conclusion

USSM's new vision for federal shared services can offer substantial benefits. Under this vision, the federal government can standardize requirements, implement shared solutions faster with lower and more predictable operating costs, and better meet demand.

Contact us:

Dave Mader
Specialist Executive
Tel: 571 858 0049
Mobile: 571 217 1214
Email: dmader@deloitte.com

Teia Clarke
Senior Manager
Tel: 571 814 7475
Mobile: 202 536 7935
Email: tclarke@deloitte.com

Chris Hamilton
Senior Consultant
Tel: 571 858 1995
Mobile: 571 379 9892
Email: chrhamilton@deloitte.com

Disclaimer