



# 5 Steps to Government **IT Modernization**



# WHY MODERNIZE?

WHY MODERNIZE? | STEP 1 | STEP 2 | STEP 3 | STEP 4 | STEP 5

IT modernization is intimidating, but it's necessary. What are the advantages of modernization?



**Create a trusted workplace** that improves health, safety, and flexibility for users



**Enhance citizen experience** and service delivery



**Lower cost** and greater efficiency



**Future-proof your agency** by planning for technology advances



**Reduce demands** on your own IT shop by moving systems to the cloud



**Improve security** and eliminate vulnerabilities inherent to legacy systems



**Take advantage of the opportunity** to leverage the latest technologies

# STEP 1: PRELIMINARIES

WHY MODERNIZE? | **STEP 1** | STEP 2 | STEP 3 | STEP 4 | STEP 5



## Develop a plan

Using an architectural approach, plot out the systems, processes and job categories that you need to modernize. Prioritize them so that you can tackle them in manageable increments.

1. Assess and inventory your IT systems; identify those that need to be replaced
2. Remember to consider licensing expenses and whether a product is still inside a support window in deciding which to update.
3. Now is the perfect time to consider your business processes. Modernization is not just swapping out a legacy system for a new one, but rethinking what systems you actually need. If there are changes that can streamline and accelerate the processes that your IT systems support, now is the time to plan them.
4. Further, if the mission of your agency has evolved recently, you might find that a different technology approach will serve the new priorities better.
5. Adopt a change-management approach and strive for full transparency so that your agency leaders and overseers understand what you are doing.

## Get leadership buy-in

You must have agency leaders, all the way to the top, fully behind your plan. They control funding and set internal priorities.

## Put cybersecurity first at every step

Build it into systems and keep it at the forefront of planning. Nothing is more important than protecting national security secrets and personal information of those who interact with your agency.

# STEP 2: START WITH THE NETWORK

WHY MODERNIZE? | STEP 1 | **STEP 2** | STEP 3 | STEP 4 | STEP 5

## What does a digital ready network entail?

The network is the backbone of everything you do in IT. It should usually be the first thing you modernize.

Replacing older switches and routers with new, smart, intuitive versions immediately multiplies security, speed and efficiency to make other steps in modernization easier.

Bringing disparate network trends and innovations together to support digital era needs.



# STEP 3: LEVERAGE SOFTWARE AND SERVICES

WHY MODERNIZE? | STEP 1 | STEP 2 | **STEP 3** | STEP 4 | STEP 5

## The benefits of a Software Defined Network

Many things that used to be hardware based are controlled by software now.

A Software Defined Network (SDN), for example, reduces agency costs through policy-enabled workflow automation.

Switches based on a Digital Network Architecture with Software Defined access turn a network from simple connectivity to a platform for delivering services.



## STEP 4: INTO THE CLOUD

WHY MODERNIZE? | STEP 1 | STEP 2 | STEP 3 | **STEP 4** | STEP 5

The cloud enables modernization without the need to “rip and replace” on-premise systems. In many cases, you can **replicate and even enhance the functionality of a legacy system by subscribing to it as a service via the cloud.**

Integrate the cloud into your migration plans. Hybrid cloud systems can blend the best of both worlds.

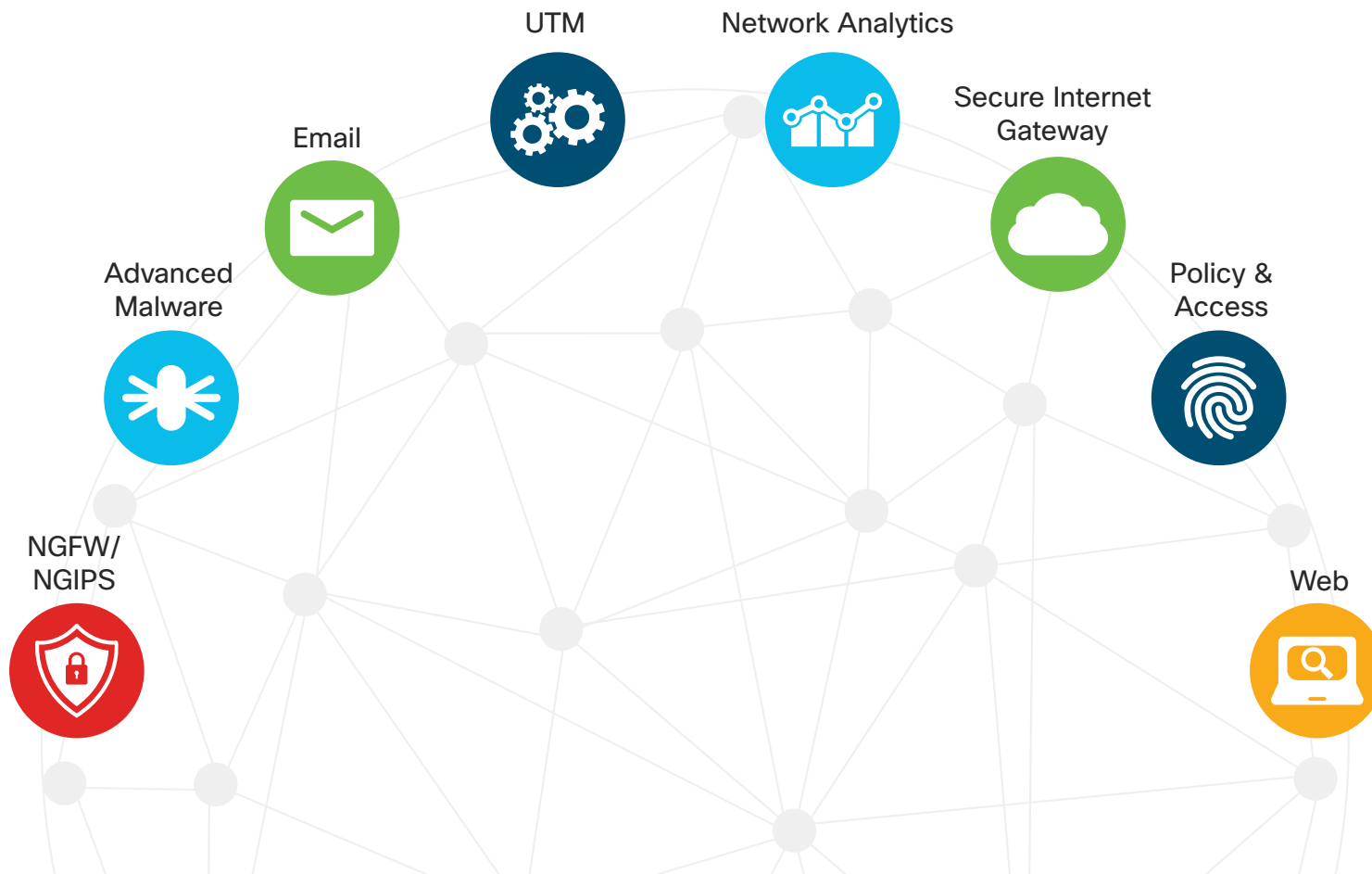
The cloud offers a secure environment and compliance with the Federal Risk Authorization and Management Program (FedRAMP) **assures a cloud offering meets federal requirements.**



# STEP 5: SECURITY FROM CORE TO EDGE

WHY MODERNIZE? | STEP 1 | STEP 2 | STEP 3 | STEP 4 | **STEP 5**

Together, these technologies **empower the advanced and agile security features needed to protect against today's threats**. By increasing visibility across your entire network and using a network-as-sensor approach, you can block malware before it enters your network, detect malicious code hiding in encrypted data and even analyze data to better understand threats and improve future defenses.



For more information, please  
visit: **[cisco.com/go/federal](https://cisco.com/go/federal)**