Resilient IT

Kieri Reference Architecture

This document describes the functionality and design for an enclave built using the Kieri Reference Architecture (KRA).

The Kieri Reference Architecture is a blueprint for creating a Microsoft 365 GCC-High and Windows 10/11 based information system. It includes scripts, technician procedures, baseline configurations, and supporting documentation to build the network yourself or with help.

The architecture and implementation are designed to be compliant with CMMC Level 2 and NIST SP 800-171 Revision 2 requirements. The enclave design is based upon the architecture and implementation that Kieri Solutions presented during their own CMMC Level 2 assessment.

To be successful with the Kieri Reference Architecture, you will need a system administrator who already knows or can learn Microsoft 365, Windows, and Azure administration.

The client organization must own a license or simultaneously purchase a license of the Kieri Compliance Documentation to use with the Kieri Reference Architecture.

Kieri Solutions subject matter experts can assist you in the following ways:

- Training (Microsoft 365, Duo, Sentinel, Endpoint Manager, AAD, Windows 10/11)
- Check-ins during your build process (explanations, getting started, quality review, troubleshooting configuration problems or changes to menus)
- Walking you through procedures and best practices the first few times
- Making sure your system security plan and other documentation are accurate

What we don't do: Kieri Solutions does not perform hands-on support for production environments. We do not offer managed services in any capacity. You will be responsible for:

- Contacting support if something doesn't work
- Building workstations, migrating users and data, and maintaining the system
- All the manual actions of compliance (account management, configuration management, self-assessment, risk analysis, etc)
- Customizations or engineering any connections to other systems

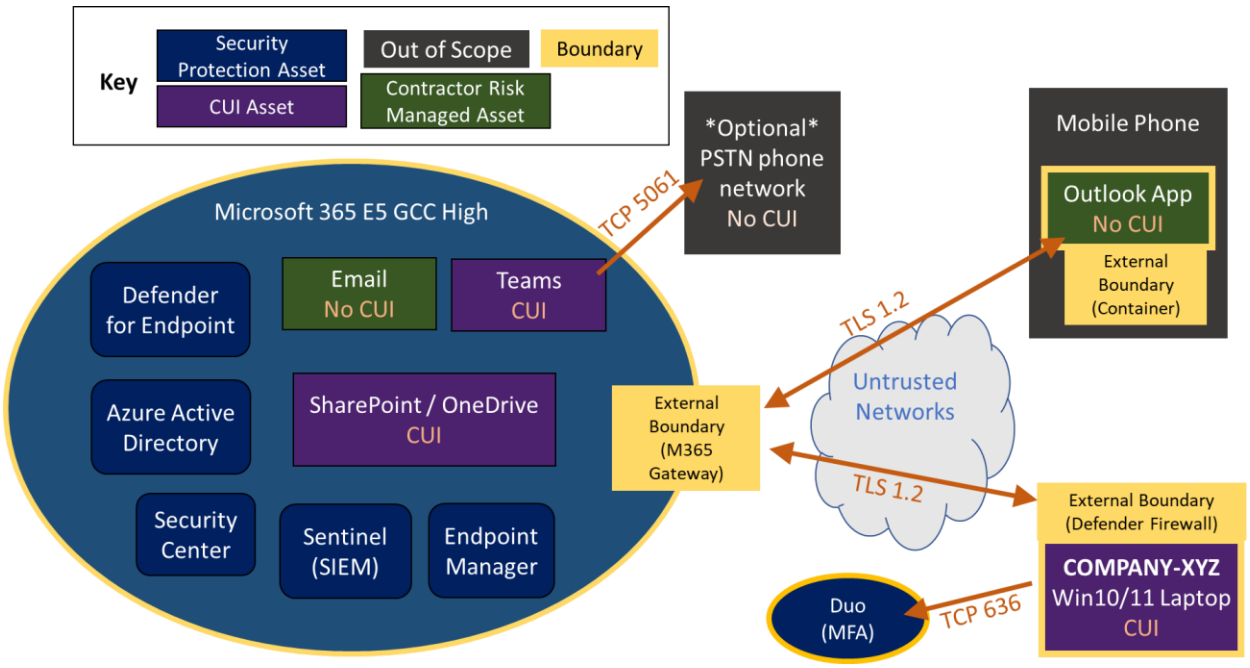
If you do not have this talent in-house, we can recommend CMMC-specialized vendors for engineering and maintenance support.

Resilient IT

1 ARCHITECTURAL DIAGRAMS

Core Kieri Reference Architecture Network Diagram

Below are the core systems described in the Kieri Reference Architecture design.



Resilient IT

Interoperability

The KRA blueprints and architectural plans only address the security of the Kieri Reference Architecture as diagrammed above. **The KRA does not include any instructions or guidance to secure systems outside of the Core Kieri Reference Architecture.**

The following interoperability diagrams discuss the use of the KRA with other systems.

These interoperability discussions do not in any way guarantee that the KRA will work with other systems. The KRA uses specific technologies (Microsoft 365, Windows, etc) which have inherent capabilities and limitations. Functionality and interoperability are limited to what these technologies can support. The KRA is not responsible for bugs, "features", vulnerabilities, or other limitations of the technologies recommended.

The KRA will not assist you in performing security for other systems. This is by design. You MUST work with a cybersecurity-qualified systems architect to develop a holistic security program for any systems used with CUI (including the KRA).

We are happy to recommend vendors who are familiar with the KRA and can design custom engineered solutions for interoperability.

Resilient IT

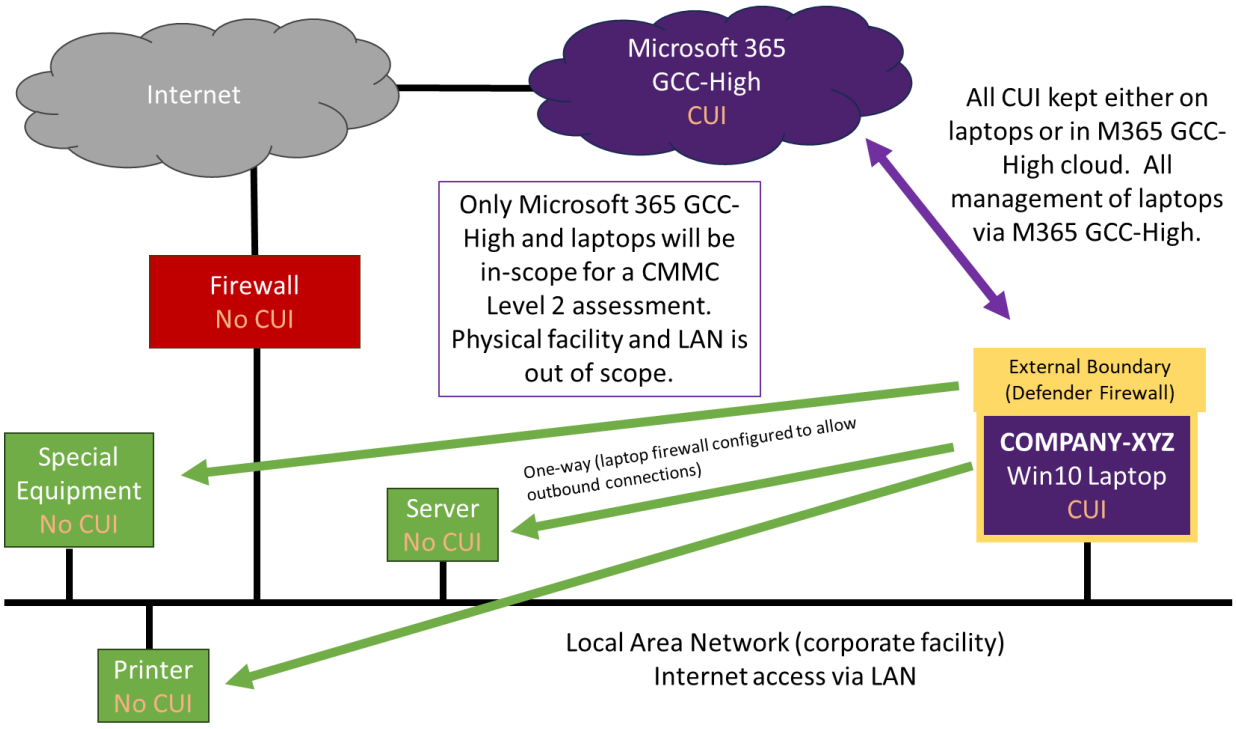
Interoperability with Commercial Network

The Kieri Reference Architecture can be used with an on-premises network that does not handle CUI.

The KRA workstation can connect to local resources such as printers, servers, and equipment across the local area network. If a non-domain-joined workstation can access a local system, the KRA workstation should be able to as well.

The on-premises network should not manage the KRA workstation in any way. The on-premises network should not connect to the Microsoft 365 GCC-High cloud (no hybrid Active Directory). The KRA workstation should not be joined to an on-premises domain. Doing any of these things will bring the on-premises network into scope.

If all CUI is kept within the KRA information system (either on Microsoft 365 GCC-High or in the workstation), the on-premises network and physical facility should be out of scope for CMMC Level 2 assessment. The firewall on the workstation and conditional access policies on Microsoft 365 GCC-High act as boundaries which keep other systems out of scope.



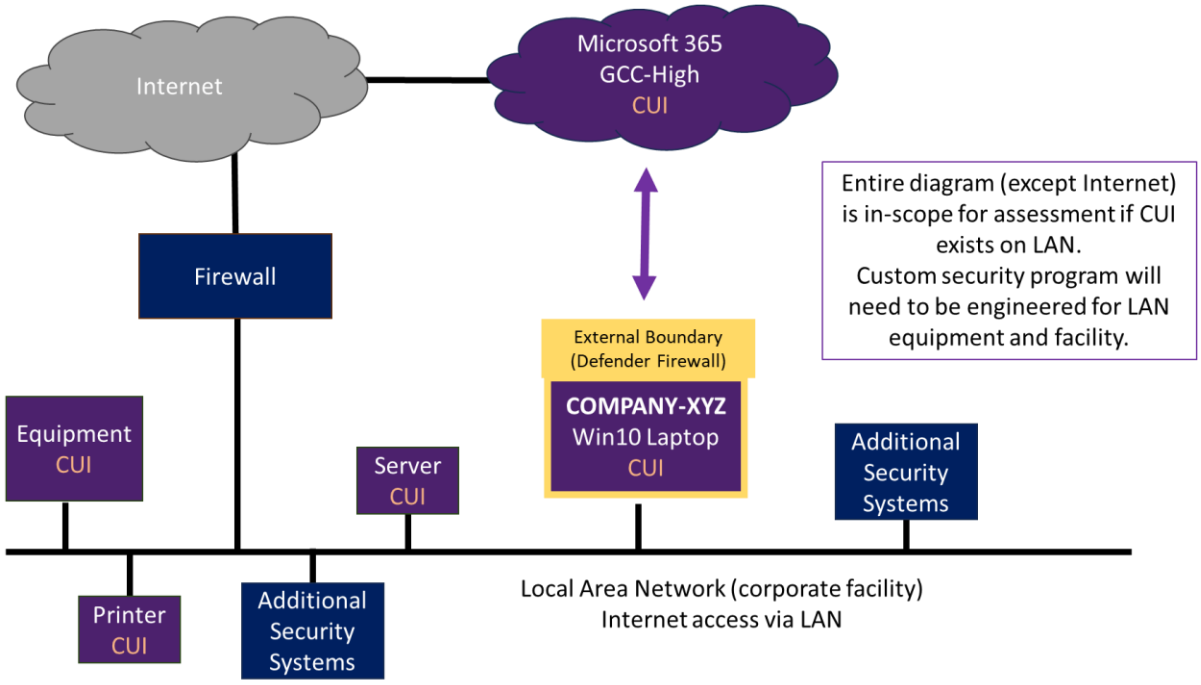
Resilient IT

Interoperability with a CUI Network

The Kieri Reference Architecture may be used with an on-premises network that contains CUI; however, it does not address the security of your on-premises network.

Microsoft 365 GCC-High and Azure Government have many tools which can be used to secure an on-premises network. For example, you can leverage Endpoint Manager, Azure Active Directory, and Sentinel to perform many requirements for on-premises systems.

The Kieri Reference Architecture does not include instructions for your on-premises systems. You will need to work with a systems architect and/or cybersecurity professional to create a plan for how these systems will comply with CMMC Level 2.

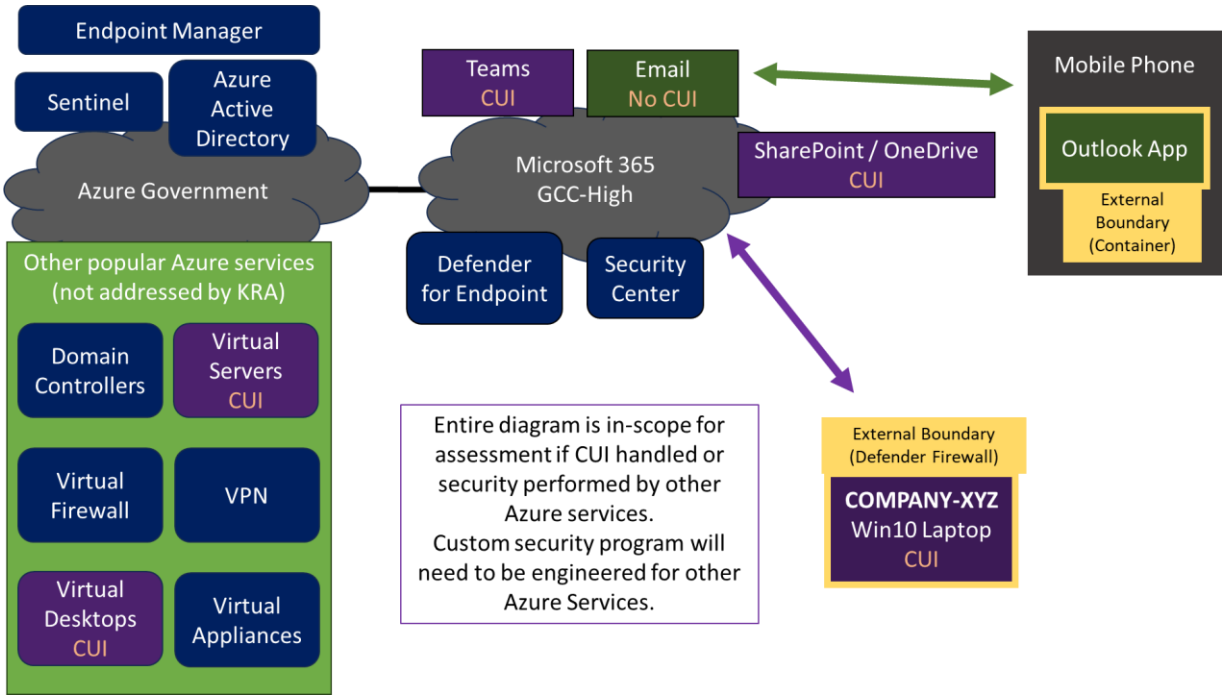


Resilient IT

Interoperability with additional Azure services

Many companies will want to incorporate additional Azure services such into their network for functionality and security. For example, Virtual Desktop Infrastructure (VDI) is extremely popular for M365 Enclaves as a means to avoid buying additional workstations. It is also popular to build virtual servers that are Domain Controllers in order to apply more granular Active Directory policies and security.

The Kieri Reference Architecture does not address the setup, configuration, or security for these additional Azure services. NIST SP 800-171 Rev.2 requirements can be met without adding this complexity, so the KRA does not use them.



Resilient IT

2 Subject Matter Expert Support

We provide expert support from Kieri Subject Matter Experts (SMEs). These SMEs will not directly manage your environment but will rather provide training and walk you through building and maintaining the KRA yourself.

Each license of the KRA comes with 10 hours of Kieri SME training and check-ins. We include this support because Microsoft 365 GCC-High tends to change its services over time (names, menu locations, and options), so we want to be available to help troubleshoot any changes.

We strongly recommend the following optional support so that you are successful:

KRA Turnkey Build: Kieri Solutions will build the core KRA for you, train you in how to maintain and use the system, customize the full set of policy and procedures you will use, and create initial evidence of compliance so that you are assessment-ready in about 4-6 months. Once we finish the build, we will hand over the keys and disable our accounts so that you are in charge once you are ready to go to production.

Build assistance: Our technicians can work with you during the build on an hourly basis to explain tricky configurations and double-check your work.

Ongoing compliance support: We can provide ongoing compliance support and self-assessment services on a monthly, quarterly, or annual basis. We can also help prepare you for third-party assessment and attend the assessment.

Note: Kieri does not perform migration of data. Kieri does not perform ongoing administrative support of the information system once it is production status (production defined as having sensitive information stored on the system or being used for any business functions). We are not a Managed Services Provider. Our goal is to enable your IT team to run a CMMC compliant system long-term through training and detailed instructions.

Contact our sales at info@kieri.com if you'd like a quote for these support options.

3 FUNCTIONALITY EXPECTATIONS

The Kieri Reference Architecture will help you configure your Microsoft 365 GCC-High tenant to meet the following functionality expectations:

All transfer of CUI will be performed via M365 GCC-High SharePoint sites, using issued accounts. Using the Government's or your prime's secure share is also acceptable.

Email:

- Email is a NO-CUI zone by default.
  NOTE: If S/MIME message-level encryption is configured (this requires purchase of digital certificates for each employee and additional process/training), you can use email to transmit encrypted CUI messages with other S/MIME enabled contractors. This option is at-your-own-risk.
- A data loss prevention policy will be enabled and configured to detect Designation Indicators on properly marked CUI documents. The policy is intended to prevent marked CUI from being emailed. This policy will delete incoming CUI emails and create an alert so that you can reach out to the sender. It will also trigger alerts if financial information or privacy information is emailed (to or from the tenant).
- Users will be restricted from accessing email unless they are using a joined and compliant Windows 10/11 workstation, OR they are using a registered BYOD phone. The phones are enabled for self-registration but an alert will be sent to the IT department if a user connects one.
- Automatic forwarding of email is disabled and will raise alarms if a user attempts to configure it.
- Web browsing to popular webmail services will be blocked.
- Email will be configured with anti-spam, anti-phish, anti-malware, and anti-spoofing protections.

SharePoint / Teams / OneDrive:

- All SharePoint sites and teams are centrally created and managed by IT. Users will not be able to create their own sites, distribution groups, or teams.
- SharePoint, Teams, and OneDrive can only be logged into from a joined and compliant Windows 10/11 workstation. Teams meetings can be joined by guests like normal, however, meetings will only be manageable from a joined and compliant workstation.

- User's desktop, documents, and pictures folders will be sync'd to the cloud automatically. Users will be able to sync and work with SharePoint files using Windows Explorer on their computer.

External access:

- You can securely share files with external people via Microsoft 365 GCC-High SharePoint.
- Your IT department will centrally approve and create accounts for external people. You will track these accounts using an expedited account management process. Your IT department will MFA, password resets, and disabling accounts for external people. These accounts don't cost anything.
- Ad-hoc (user-approved) file sharing external to your organization will be disabled.

Microsoft 365 GCC-High general:

- Banner warnings, lockout thresholds, multi-factor, and other configurations will be made throughout Microsoft 365 GCC-High according to recommended security best practices.
- Azure Active Directory-based MFA will be enforced on all accounts. Users must be willing to receive SMS text messages or Microsoft Authenticator prompts to log on.

Audit and Incident Response

- Audit logging and security alerts will be configured in Microsoft 365 Security Center and Azure Sentinel.
- Azure Sentinel incurs cost on a usage basis. Typical enclave deployments cost $5- $20 per month.
- Your Azure Sentinel will email your IT department by relaying emails from Azure Logic App. Typically, a low-cost or free email account is used for this relay, such as free email provided by a website host.
- Microsoft 365 Security Center will be configured to capture activity from Windows 10/11 workstations.

Windows 10/11:

- Endpoint Manager (previously called Intune) will be configured to deploy necessary security policies and baselines to Windows 10/11 workstations.

- Windows 10/11 workstations will be extremely locked down. Users will not be able to install software or execute downloaded apps. The firewall will be enabled in deny-by-default mode at the workstation. Removable media will be disabled.
- Printing from Windows 10/11 will be disabled by default. If a document that needs printing is not sensitive, it can be emailed to a corporate or personal account and printed from there.
  NOTE: You can allow printing, but you will be responsible for security of the printers, related network, and facilities (including home security) if this is done. This option is at-your-own-risk.
- Non-essential programs and functions will be disabled.
- Duo MFA will be enabled for all logons to Windows 10/11. Users must be willing to install and use the Duo App on their phones. We are expecting an update to Windows Hello for Business in early 2024. Depending on testing, we may be able to start using Windows Hello for Business and the Microsoft Authenticator App instead of Duo.
- You will need to create install packages for your business applications in Endpoint Manager. Because we don't know your business applications, the KRA does not include instructions for how to do this. However, Kieri consultants can teach you how this works and there is public training available for the topic.
- FIPS protection for CUI in transit and storage will be enabled throughout the environment. This can cause some applications, such as QuickBooks, to not work. Ensure your business applications are functional with FIPS Mode enabled (or ensure you do not need the applications on your KRA workstations) prior to accepting this project.
- Privileged accounts will be able to support the workstations and install one-off software. We include instructions for a local workstation admin account that can be used by remote users to troubleshoot their own computer or perform changes under supervision during a Teams web conference. The KRA does not include capability to remote-control workstations without user interaction.
- You will need to track all workstations in the Hardware Inventory. All workstations will be built following a PC Build Procedure which takes about 2 hours (spread across 1-2 days) by an IT person.

Local networks and facility:

- The workstations can be connected to a local network in your facility. Enclave workstations will have strong firewalls which prevent your corporate network from accessing them.
- If you have a server (such as a license server) that needs to be accessible from the workstations you will need to configure the firewall rules on the workstations to allow access. We can help show you what to do for this.

- You are responsible for security of the facility and local network. In general, the local network and facility should be considered “out of scope” as long as enclave workstations are fully locked down, firewalled, cannot print, cannot connect to media, and all CUI is kept inside the workstations and M365, with no physical copies of CUI.
- You are responsible for security of other devices in-scope for CMMC (such as Operational Technology).

Record keeping:

- You are expected to create an IT Department SharePoint site and deploy the configuration management and service management databases recommended by the KCD / KRA.
- You will update the lists and records to match the work that is performed during the enclave build process.
- You will be responsible for managing compliance documentation, putting copies of scripts and other build files into the IT Department SharePoint, and verifying that the System Security Plan and procedures match the exact policies and configurations you created.
- It is incredibly important that you start record keeping as soon as possible (ideally before starting the KRA build) so that you have evidence to show your assessors that you are performing compliance processes correctly.

Manual activities for compliance:

- You will be wholly responsible for performance of all policy, procedures, maintenance, ongoing monitoring, and other activities related to CMMC compliance. The Kieri Compliance Documentation includes a training library, free check-ins, and monthly Q&A webinar to help you with these manual activities. Kieri can also provide consulting / training / quality review for these activities.

Shared Responsibility Matrix:

- Kieri Solutions has no shared responsibilities for the KRA. This is a “do it yourself” set of documentation and training. We can advise you and help prepare you for assessment, but we will not have administrative rights on your production system and we perform no security function on your behalf.
- The specified cloud vendors (Microsoft 365 GCC-High and Duo) meet requirements for FedRAMP Moderate or High equivalency. We recommend reaching out to both vendors to obtain their FedRAMP package which includes System Security Plan and Shared

Responsibility Matrix. We also recommend reviewing the [Microsoft Product Placemat for CMMC 2.0](#).

- You are responsible for ensuring that all 800-171 and CMMC Level 2 requirements are performed (by internal staff, cloud vendors, or third-party support) for your organization as a whole. You are fully responsible for security of your Windows workstations and partially responsible for security of your Microsoft 365 GCC-High tenant.

4 License and Services

Below are estimated costs related to building and maintaining a Kieri Reference Architecture.

Licensing	
Kieri Compliance Documentation license with 12-month subscription to training and updates	$5,200
Kieri Reference Architecture license with 12-month subscription to training and updates (includes up to 10 hours of engineering support)	$9,700

Optional support	
Build support: Build it yourself with help: Kieri's engineer will meet with you to get you started, train you on essential procedures and maintenance, quality-review your work, and customize your compliance documentation. (40 hours)	$12,800
Turnkey build: We build it for you, hand-off the keys, then give you driving lessons. Kieri's engineer will configure your tenant and core Reference Architecture build. We then train you on essential procedures and maintenance, test functionality, and customize your compliance documentation while gathering evidence. Intended to be audit-ready (core KRA) by the end of the project. Only available for pre-production environments.	$32,800

Yearly subscription fees	
Renew Kieri Compliance Documentation subscription for 12 months (access to latest training and updates, 3x30-minute assessor check-ins)	$1,800
Renew Kieri Reference Architecture subscription for 12 months (access to latest training and updates, up to 10 hours of engineering, self-assessment, and audit readiness review)	$4,000

5 YOU WILL NEED TO PURCHASE….

As part of the build instructions, we will provide you an itemized list of software and hardware to purchase.

6 HIGH LEVEL TIMELINE

Recommended timeline:

1. Review and customize your Kieri Compliance Documentation policies, administrative processes, and user agreements with the assistance of a Kieri subject matter expert.
2. Start a change request to create the KRA Enclave and approve the change in a Change Approval Board meeting with the assistance of a Kieri subject matter expert.
3. Have your initial users perform the access request process and track authorizations, user agreements, training, and background screening.
4. Purchase 2+ licenses for Microsoft 365 GCC High
5. Purchase 5+ licenses for the FedRAMP version of Duo MFA (typically 10 minimum)
6. Establish initial administrator accounts for Microsoft 365 GCC High, Azure Government, and Duo MFA.
7. Purchase 2+ Dell laptops for use with the enclave.
8. Identify one Android phone and one iPhone for use with the enclave.
9. Secure a new domain name which is not being used in your production network and configure DNS settings to enable email and authentication to the new M365 tenant.
10. Follow the provided instructions to configure Microsoft 365, Azure Sentinel, Endpoint Manager, and Duo MFA for use.
11. Test the automated deployment and configuration status of your workstations.
12. Create an IT SharePoint Site and establish record-keeping locations, such as Change Database, Hardware Inventory, Account Management database, SOFTWARE folder, and WORK_LOGS folder.
13. Fill out required information in each of the databases and folder locations so that records of your environment are accurate.
14. Perform appropriate maintenance activities per the Cybersecurity Maintenance Checklist.
15. Perform monthly Change Approval Board meetings.
16. Uphold cybersecurity policies and perform procedures recommended by the Kieri Compliance Documentation.
17. Perform a self-assessment with the assistance of a Kieri subject matter expert to verify that cybersecurity controls are effective in the enclave.
18. Only at this point will you migrate data and production capabilities to the enclave.

Resilient IT

7 How much time does this take?

Hours are estimated based on a cloud engineer / senior systems administrator who has performed similar tasks before.

Order	Task	Level of Effort	Average duration
1	Purchase cloud subscriptions	6 hours	30 days
1	Purchase and update DNS to point at M365 Tenant	5 hours	5 days
1	Purchase laptops	4 hours	15 days
2	Customize KCD policies, user agreements, administrative processes, approve for use	15 hours	15 days
2	Change Request / Account Requests	6 hours	3 days
3	Configure M365[1] tenant general settings (Security Center, Data Loss Protection, Audit Policies, AAD)	10 hours	5 days
3	Configure Azure Sentinel and push alerts	8 hours	5 days
3	Configure Endpoint Manager settings and Duo[2]	20 hours	15 days
4	Test building workstations, BYOD phones, and functionality	20 hours	5 days
5	Update records (software inventory, hardware inventory, change management, account database, work logs, maintenance, procedures)	16 hours	10 days
5	Perform all maintenance and compliance tasks first time, and as scheduled weekly	20 hours	30 days
6	Full review of SSP and self-assessment	20 hours	15 days
	Critical path	**150 hours**	**4 months**

Once these steps are complete, you may start migrating data and users to the new enclave.

[1] Microsoft®, Azure®, Windows®, Windows 10®, Windows 11®, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

[2] Duo ® is a registered trademark of Duo Security, Inc. in the United States and/or other countries.

Resilient IT

For budgeting purposes, you should expect the following internal labor and costs to maintain your core KRA environment:

Re-occurring costs (estimated internal costs)	
Workstations	$300 / year / user
Cloud Licenses (per user) *Kieri is not a reseller*	$1200 / year / user
Calltower (optional - dial-in to meetings)	$3000 / year (for small biz)
Other costs (estimated internal costs)	
Helpdesk support compliant to CMMC Level 2 (about 20 hours per year per user)	$2k / year / user, $20k per year min
Cybersecurity program compliant to CMMC Level 2 (about 10 hours per year per user)	$2k / year / user, $30k per year min
CMMC Level 2 assessment *Kieri Solutions does not assess the KRA*	$20-30k / 3 years for core KRA