TESSERACT SECURE

Secure Compliance, Simplified.

Welcome to Tesseract Secure: What to Expect

Your Path to Compliance Starts Now

Welcome to Tesseract Secure

Welcome to Tesseract Secure! We're excited to help you achieve CMMC compliance with our expert-led, flexible, and affordable solution. This document outlines what you can expect during the onboarding process, ensuring a smooth and valuable experience.

Deployment at a Glance

Onboarding Task Key

Indicates work being done by the Ardalyst Customer Success Team

Indicates work to be done by you, the customer.

Indicates a document or activity done by Ardalyst that needs to be reviewed and/or approved by you, the customer.

Your Compliance Journey

Contract Signed

This phase marks the formal beginning of your partnership with Ardalyst. Once the contract is signed, internal notifications are triggered, and responsibility is handed off to the Customer Success team to begin coordinating onboarding logistics.

- Your Account Executive will alert the Customer Success Team
- You'll receive a welcome email with your next steps
- The Customer Success Team will email you to schedule your Customer Kickoff
- Accounting will submit your invoice for payment
- Please remit payment as soon as possible to begin license procurement and ensure your onboarding remains on schedule.

Customer Kickoff

The Customer Kickoff is your first official touch point with the Customer Success Team. This meeting set expectations for your onboarding experience and your overall program, confirm key details like user, domains, and goals, and maps out your unique timeline and responsibilities.

- Dive into your onboarding plan, milestones, and what you can expect
- Explain next steps and customer expectations
- Walk through the Change Management process
- Align on user counts, domains, and migration preferences.
- Identify who needs support portal credentials and Knowledge Hub library access.
- Following kickoff, the Ardalyst Service Desk will send invites to identified users to access our support portal.

Program Activation

Your environment is actively provisioned. Microsoft GCC High licenses and Azure subscriptions are ordered and the GCC High tenant is created and configured. Planning for migrations (if applicable) also begins here.

- GCC High tenant provisioned
- Azure subscription is procured and configured within the tenant
- Admin and user accounts are created
- Program governance documentation begins
- Migration planning begins (if applicable)

Documentation

To meet the CMMC and NIST 800-171 requirements, a full set of compliance documentation is developed for your program. This includes system security plans, acceptable use policies, incident response plans, and more. Ardalyst works closely with you to gather the necessary inputs, ensure policies reflect your real-world operations, and prepare you for eventual assessments.

- We'll build all required documentation for your program:
    - Scope Enclave and CUI Flow Diagrams
    - Risk Assessment
    - Cybersecurity Policy Manual (CPM) reflecting Tesseract Block selection
    - Incident Response Plan
    - Acceptable Use Policy
    - Change Management
    - System Security Plan (SSP)
- Review and sign off on key documents

Baselining

This technical step establishes your cybersecurity controls in alignment with the compliance framework. Ardalyst configures security tools like Microsoft Defender, Intune, Azure Sentinel, and more. These actions ensure the environment is secure, monitored, and compliance from day one.

- GCC High tenant is configured to the Tesseract Secure security architecture
- Configure Microsoft tools to lock down your environment and ensure you meet security standards
    - Microsoft Defender Suite (XDR, Office, Endpoint, Cloud Apps)
    - Sentinel SIEM Deployment
    - DLP & Sensitivity Label Setup
    - Privileged Identity Management (PIM)
    - Conditional Access and Policy Framework Setup
    - Intune Setup (If Applicable)
    - Device Enrollment and Validation (If Applicable)

Get a Jump on What's Next

Get a Jump on Customer Kickoff

Confirm Your Domain: We'll ask you to confirm which domain you plan to use for your Tesseract Secure environment. Most organizations choose to procure a .us domain to visually distinguish to your end customers that you are operating in a compliant environment, but it is entirely up to you! If you are not purchasing a new domain but rather want to migrate your existing .com or other domain to the Tesseract enclave, please let your Account Executive know. Having your new domain purchased and the Point-of-Contact (POC) identified ensures that secure email can be set up as quickly as possible.

Identify Your Users: Start thinking about who needs access to the secure environment and what level of access each person will need (Web, Cloud, or Kiosk). Who on your team will need access to create cases with the Ardalyst Service Desk and access the Ardalyst Knowledge Hub? Having this list ready allows us to provision accounts much faster.

Get a Jump on Program Activation

Documenting Users: Access the provided user import template to create a list of user accounts that need to be created for M365. Please leverage the support portal to upload to Ardalyst (credentials will have been shared after the Customer Kickoff meeting).

Get a Jump on Documentation

Review and Approve Policies: Review the Acceptable Use Policy and Incident Response Plan.

Schedule IR Tabletop: Coordinate with internal stakeholders to schedule your hour-long Incident Response tabletop exercise with Customer Success.

Document User Training: Based on the strictness choices you make for training, your organization will be responsible for implementing role-based, security awareness and insider threat training. We provide an Advisory Article on training with links to course options you can use in completion of these Assessment Objectives.

Document Background Checks: Ensure that implementation matches the strictness selection you make, and your organization knows where evidence is documented in support of this requirement (typically by Human Resources).

Get a Jump on Data Migration (If Applicable)

Identify What Needs to Be Migrated: Take inventory of the data you'd like moved into your Tesseract Secure enclave, such as which users or departments need data access, which folders, file shares, or OneDrives contain CUI or sensitive data, and if any mailboxes or shared drives should be included.

Clean Up Old or Unneeded Files: Migration is a great opportunity to declutter. Consider archiving or deleting outdated files, removing duplicates or unused folders, and renaming files and folders for easier navigation post-migration.

Organize or Classify Sensitive Data: If you already know which files include CUI, flag them or place them in dedicated folders to help assign proper sensitivity labels, align your DLP (Data Loss Prevention) policies, and ensure compliance boundaries are respected.

Staying Assessment-Ready

Tesseract Secure is designed to make cybersecurity and compliance easier - but staying ready for a CMMC assessment still requires a few good habits. The good news? Most of the heavy lifting is covered through your Tesseract Secure Plus Service. Here's what we suggest to help you stay sharp and assessment-ready.

Lean on the Tesseract Secure Plus Service: Your Plus Service includes expert teams who monitor your environment every day, manage your system baseline and secure configurations, keep documentation up to date, and investigate and respond to security alerts. You're not alone!

Keep Us in the Loop: While we handle the technical details, you can support long-term success by notifying Ardalyst when roles change or new users are added or removed, following Acceptable User Policies and encouraging your team to do the same, and flagging unusual activity or user concerns through cases to our Service Desk

Keep Your Documents Fresh: We'll manage and maintain your program documentation but if your business structure, tools, or operations change, open a Change Control Request with the Ardalyst Service Desk so we can update them. The faster we know, the faster we keep your compliance airtight.

Support Resources

You've chosen a simple, focused path to compliance - and we're here to make it seamless.

- **The Ardalyst Support Portal:** Submit cases for Customer Success to view and address, track, and manage your cases. Use the portal to submit cases to your Ardalyst Operate Team, see security cases, ask us compliance questions, conduct change management, add licenses and more.
- **Knowledge Hub:** Accessed through the Support Portal, search the extensive library of self-service articles to leverage our expert's How-To, Troubleshooting, and Advisory Articles.
- **Support Contact:** While the fastest way to reach the Service Desk is always to open a case, you can also email Ardalyst at support@ardalyst.com or give us a call at (833) 682-8270.