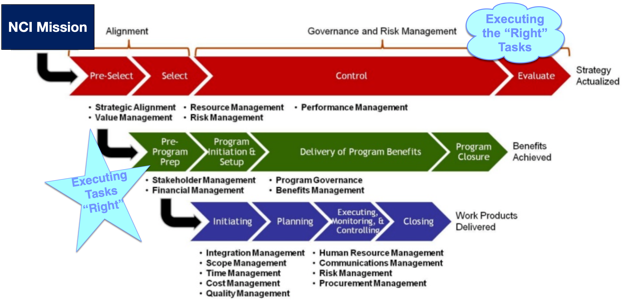
5.1 - TASK 1 – TASK ORDER MANAGEMENT

Task order (TO) management is the process of overseeing all the tasks associated with the performance and delivery of the technical and functional activities necessary for the management of the activities under the SOW, including oversight of all tasks provided by our personnel and subcontractors. The DIFZ Team’s task order management methodology entails working closely with the NCI COR to identify stakeholders, priorities and schedule, and employs industry best practices such as Project Management Body of Knowledge (PMBOK), Capability Maturity Model Integration (CMMI) and Agile. We will define our task management approach to efficiently meet NCI requirements through an Abbreviated Task Order Management Plan (TOMP) that will be delivered to the NCI COR five (5) days after task order award. The TOMP will briefly describe our technical approach, resources and management controls that will be utilized to meet the cost, performance and schedule requirements throughout task order execution.

The essentials of this process may be ongoing, such as in the consistent delivery of products to customers under the terms of a contractual agreement, or may have to do with the structuring and execution of tasks related to the internal function of a specific NCI mission operation. Having performed similar work for our clients, we recognize that the SOW tasks/subtasks are interconnected and interdependent. We understand that this will require our team to collaboratively work together and with various NCI stakeholders, to approach this work holistically. Exhibit x presents the interconnectedness between the tasks/subtasks and our understanding of the primary objectives for each task/subtask.

Based on ITSM, Team DIFZ provides a service catalog driven task order management approach that facilitates our efficiently managing the end to end information technology life cycle to address NCI’s complex needs. This innovative approach solution allows use to implement a set of standardized, product catalog-based business processes aligned to total customer satisfaction and 100% compliance with the SOW. We are able to assume responsibility to meet cost, performance, and schedule requirements through task execution, with regular reporting to ensure communication of results. “Stress tested” at other NIH institutes, this solution supports complex task orchestration, subtask decomposition, dependency management, NCI, agency, and federal standards-based integration, human resource management, risk mitigation handling, and automation of many manually intensive activities.

**Exhibit x. Integrated Approach to Managing this Task Order**— driven by the needs of NCI stakeholders, the DIFZ Team approach is both transparent and process-based.

Project related artifacts (e.g., meeting agendas and notes, action items, deliverables, risk register) and an updated schedule will be made available to the NCI COR and relevant technical contacts. Exhibit x depicts our proposed project schedule and high-level work breakdown structure, and outlines the project activities and deliverables within the period of performance. As part of our comprehensive communications plan, we will meet with CTEP personnel within two hours’ notice at either NCI or our own meeting location — or by remote means (WebEx, Microsoft Teams). The proposed project schedule in the following exhibit will provide the NCI COR and CTEP with appropriate time for feedback and review and will ensure proper oversight and execution of the project tasks. The DIFZ Team will review and validate this proposed schedule and get approval from the NCI COR upon contract award.

**Exhibit x. Work Breakdown Structure WBS and Project Schedule**

| **WBS** | **Task Name** | **SOW** | **Duration** |
| --- | --- | --- | --- |
|  | **C-88611-SB – Cancer Therapy Evaluation Program Informatics & Computer Support** |  | 365 days |
| 1 | **Task 1 – Task Order Management** | 5.1 | 365 days |
| 1.1 | **Planning and Project Oversight** | 5.1.1 | 30+ days |
|  | **Task 1 is on-going over the life of the effort** |  |  |
| 2 | **Task 2 – IT Infrastructure**  **and System Security (SOW 5.2)** | 5.2 | 167days |
| 2.1 | Data Center Services | 5.2.1 | 365 days |
| 2.1.1 | Requirements and service | 5.2.1.1 | 365 days |
| 2.1.2 | Software | 5.2.1.2 | 365 days |
| 2.1.3 | Facility Safety | 5.2.1.3 | 365 days |
| 2.2 | System Security | 5.2.2 | 365 days |
| 2.3 | System Backup and Disaster Recovery Management | 5.2.3 | 365 days |
|  | **Task 2 is on-going over the life of the effort** |  |  |
| 3 | **Task 3 – Operations and Maintenance** | 5.3 | 365 days |
| 3.1 | Help Desk | 5.3.1 | 365 days |
| 3.2 | Incidents (Break/Fix Support) | 5.3.2 | 365 days |
| 3.3 | Configuration Management | 5.3.3 | 365 days |
| 3.4 | System Manuals and Training | 5.3.4 | 365 days |
| 3.5 | IT Planning, Reports and Data Calls | 5.3.5 | 365 days |
|  | **Task 3 is on-going over the life of the effort** |  |  |
| 4 | **Task 4 – Information Management** | 5.4 | 365 days |
| 4.1 | Data Repositories/Warehouse | 5.4.1 | 365 days |
| 4.2 | System Integrity and Interoperability | 5.4.2 | 365 days |
| 4.3 | 508 Compliance Requirements | 5.4.3 | 365 days |
|  | **Task 4 is on-going over the life of the effort** |  |  |
| Option A | **Option A: Hardware Sustainment**  **and Backed-Up Data Storage** |  | TBD |
| Option B | **Option B: Primary DC Migration** |  | TBD |
| Option C | **Option C: Secondary DC Migration** |  | TBD |
|  |  |  |  |
| T-1 | **Transition-in** |  | 90 |
| T-2 | **Transition-out** |  | 90 |

Ongoing planning and scheduling for each of the related tasks include updating the above schedule for completion of each phase, coordinating assets and labor to manage this part of the process, and implementing the PMBOK framework that is both productive and efficient for the completion of essential steps within each task (referenced by WBS numbers corresponding to the SOW. As part of task order management, this planning evolves to help to further define what activities take place at each step of each process.

The third phase of task order management involves the actual execution of the planning. During this phase, Team DIFZ monitors the production process to make sure efficiency is maintained at high levels, while slippage is also kept to a minimum. During this phase, our management process (see section \_\_\_) may also involve refining operations and management protocols and procedures as a means of making tasks more cost-efficient. This also helps to provide a means of reviewing specifications and make sure the products are within the required quality standards, as we describe in our Quality Control Plan (QCP).

As communication is key to the success in any complex endeavor, Team DIFZ will provide a point of contact for each of the top-level WBS/task areas. To ensure an open dialogue, understanding of responsibilities, and clear lines of responsibility, Team DIFZ will deputize the Program Manager as the overall single point of contact. See the following exhibit, Organization of Project and Lines of Communication.

**Exhibit x. Organization of Project and Lines of Communication**

In carrying out NCI’s objectives, we will ensure all services provided use Information Technology Infrastructure Library (ITIL) v3 and International Organization for Standardization (ISO) 20000-based frameworks, and will help NCI with any change management steps needed to fully realize the potential of these best practices. Team DIFZ will ensure the desired outcomes are achieved through measurable service level metrics in line with our QCP tied to the government's QASP and performance objectives, and associated reporting and surveillance methods. We will promote process and quality management methodologies that produce repeatable positive outcomes, encourage the incorporation of lessons learned, reduce service delivery time, costs, and minimize defects, and provide the government greater visibility into the status and health of ongoing operations and maintenance initiatives and system development initiatives.

Our team’s risk management includes front-end planning of how major risks will be mitigated and managed once identified. Therefore, risk mitigation strategies and specific action plans will be incorporated in the final Project Management Plan (PMP). Exhibit x outlines anticipated obstacles (risks) and mitigation strategies. Team DIFZ understands some risks, once identified, can readily be eliminated or reduced. However, many risks are much more difficult to mitigate, particularly high-impact, low-probability risks. We ensure risk mitigation and management are long-term throughout the project by incorporating periodic risk reviews into our status updates.

**Exhibit x. Potential Obstacles and Mitigation Strategies**

| **Potential Obstacle** | **Mitigation Strategy** |
| --- | --- |
| Delays in project schedule due to logistical issues. | To minimize impact on the schedule, it is recommended that NCI identify key stakeholders and are made available from project start. One way to sustain stakeholder commitment is to have effective governance. We understand the NCI governance structure and know that the process will work to bring together different stakeholders on a regular cadence to keep them committed, to seek their counsel, and to gain their support for future direction. |
| The team’s staff not being able to access NIH resources due to on-boarding delays that impact project schedule. | A critical element for successful implementation is having people with the skills and experience to execute this effort. The DIFZ Team has worked with several NIH ICs and the key members of the team already have NIH badge/account credentials that will mitigate any project schedule impacts due to on-boarding delays. |
| NCI stakeholders, system owners, and others involved in key systems have many demands on their attention. Those driving change often have little or no excess capacity and time to undertake yet another project to execute the change. | We have handled this problem in the past when doing research on Academic Medical Centers by being persistent with group outreach and follow up and by offering flexibility (video conferencing, web-meetings) with regard to interacting. We understand change requires extra effort; all too often, though, these efforts are additive to existing demands. Our team will minimize additional workload by automating activities so that scientists can more easily focus on their research, and less on administrative functions. |

Evaluation for Full Performance and Acceptability of Work — At each major milestone, the work to date will be evaluated primarily on how well it helped to satisfy the objectives of the SOW. Specifically, each milestone will be evaluated by the NCI CO and CTEP with respect to: accuracy, completeness, assistance in answering the desired questions, and in uncovering unexpected information. Acceptability of the work will be measured by the level of understanding it provides NCI regarding their stakeholders’ needs and use-case tasks they would ideally like to be able to perform.

Team DIFZ promotes a wide range of strategies to ensure the goals associated with each of the tasks are met. This includes ongoing employee training, evaluation of processes and production methods, assessing help desk ticket quotas, and even fine tuning SOPs from time to time. From the Team DIFZ perspective, task order management is an ongoing activity — driven by standardized processes — that begins with the commencement of the contractual agreement and only ends once the contract is completely fulfilled.

5.2 TASK 2 – IT INFRASTRUCTURE AND SYSTEM SECURITY

The DIFZ Team brings experience working with a wide variety of Federal Agencies to implement IT infrastructure and information security programs. The examples following, from Digital Infuzion and our teaming partners, demonstrate our experience and extensive IT security expertise and resources that we have deployed in Federal contracts. For SOW 5.2.1  Data Center Services, in addition to the core services for interface with the NOC, we will implement NCI’s security program in compliance with NIH and NCI directives, HSPD, and FISMA. Primarily, the DIFZ Team will undertake implementation and upkeep of CTEP-ESYS data center components, protection of the data and respective applications from internal and external threats, and establish continuity of operations mechanisms for efficient restoration of CTEP operations after a security incident. Our security approach relies on risk assessment in keeping with NIST’s recommended approach, proactive monitoring, and the formation of quick-response teams with forensic expertise so that we can mitigate the fallout from any potential security breach.

So that we maintain the CTEP applications within the NIH or NCI data center (or NCI managed cloud environment if applicable) following the Data Center hosting requirements at all times and ensure NCI systems comply with applicable federal laws, our team will build out a regulatory and procedurally compliant contingency plans as part of our security and DR efforts. To do this, we will craft a security plan that meets or exceeds the following requirements: HHS Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-series (e.g., 800-53, 800-63), Security and Privacy Controls for Federal Information Systems and Organizations; Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and other applicable federal laws, regulations, NIST guidance, and HHS, NIH, and NCI Departmental policies.

Team DIFZ has experience with NIH legacy network/data center consolidation efforts as well as transition to cloud services; cloud computing; experience with other NIH enterprise solutions/databases such as \_\_\_\_\_ applications and \_\_\_ database management systems. Additionally, expertise with Microsoft Office (i.e., Excel, Word, PowerPoint); verbal and written communication skills to clearly communicate with NCI NOC POCs; and having a self-directed ability to work solo and collaboratively in a team environment or with NCI management, peers, and customers are essential. Team DIFZ understands NIST 800-series frameworks for security self-assessments, having conducted A&A/C&As and other audits at several federal agencies. We will recommend processes that have been tried-and-tested so that formal written documentation is available to notify the data center of any changes in needs or requirements. Through the help desk, we will provide current contact and escalation information for the Federal Sponsor of any applications and the Technical Project’s lead. This is an automated process, when a ticket is opened. As communication is a cornerstone of the Team DIFZ approach to SOW 5.2.1.1 Requirements and Service, we will convene daily standup meetings so that our team consolidates all change requests and documents outstanding issues; we will then notify the data center of any changes in needs or requirements. We will submit service requests as per data center policy, and not call the on-call phone number for general support, reserving its use for critical emergencies.

To ensure SOW 5.2.1.2 Software is provided and maintained as necessary for the CTEP-ESYS environment and services not provided by the data center, Team DIFZ will integrate support with a well-documented configuration management process, patch management, and version control. Understanding what applications are in the environment is the cornerstone, and Team DIFZ will update the government’s inventory of applications, ensuring accurate information about licenses, deployment environments, versions, known vulnerabilities, and the user base for each. Software is central to NCI, for researcher support. Managing the software asset requires processes that are easily adaptable and robust.

Team DIFZ will maintain and update government developed software, COTS software configurations, and software systems. We will implement software configuration management (CM) procedures to provide a uniform approach to supporting CTEP-ESYS and other custom developed systems. We will assign a software configuration manager to educate organization stakeholders on CM “best practices,” develop and maintain CM procedures and work instructions for each product assigned. We will only employ software that has vendor or community support, per HHS policy. The DIFZ team will establish release baselines and work with the development and data center teams in administering CM repositories. The Team DIFZ process for maintaining and updating software includes the development and maintenance of artifacts following proper version control procedures using CMMI-L3 compliant CM processes and work instructions. We will work with the NCI governance body for reviewing and approving change requests under CM procedures and work instructions.

Team DIFZ will comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes (see https://www.hhs.gov/sites/default/files/eplc-policy-dec- 2016.pdf), and HHS Enterprise Architecture requirements to ensure information is appropriately protected. We acknowledge that all information systems development or enhancement tasks will follow the HHS EPLC framework.

Our overall development methodology is hybrid of a waterfall approach modified with Agile practices — as applicable to the complexity of the requested development effort or enhancement, as well as adapting a more iterative agile approach for change requests needed on an expedited basis. building and maintain in stable and secure applications. As we discuss under CM, we will document CTEP-ESYS equipment configuration and specifications. Our systems engineers will manage all CTEP-ESYS equipment including shut down and restarts and provide remediation (tier 3) for all CTEP-ESYS application and service issues.

**Exhibit x. Making Changes to Software**. The development process needed to support minor enhancements and defect resolution mirrors a larger system life cycle, but is scaled back depending on the scope of specific enhancements.

| **Type of Change** | **Methodology** |
| --- | --- |
| **Minor Enhancement** | |
| Enhancements that require less than 40 hours of labor and are therefore scheduled as part of normal support operations. | Follow all phases and documentation requirements of the normal SDLC. |
| **Bug Fix** | |
| Small software patches to correct defective code. | Include only the Version Description Document (VDD). |
| **Proof of Concept** | |
| Development of prototypes to validate new technologies, architectures, and business requirements prior to commitment of significant resources. | Conduct abbreviated requirements and development phases of the SDLC. Requirements must be documented, but do not require a formal Systems Requirement Document. Example: create site-flows / web pages to describe how the application would work in an informal way. |

To perform all application deployments, Team DIFZ will follow NCI procedures for rolling out a tested and approved application. Deploying software to production correctly is a challenge. Bad deployments can lead to delays and even downtime. Being in charge of a deployment process is a big responsibility as well as a huge challenge. Modern software deployment involves many moving parts across the organization and its toolset. For this, we will document the release to production with a plan. Creating a deployment plan is an opportunity to get insight from all stakeholders. Once the plan is in place, it provides crucial information and instructions for the entire deployment. Plans may involve both manual and automated testing at each deployment stage. Risk analyses, checklists, responsibilities, and contact information for each stakeholder also play a role. The plan should be reviewed and approved by all stakeholders.

As discussed under CM, we have demonstrated that Team DIFZ recognizes how coherent versioning and release notes contribute to good documentation, especially as we plan on the use of a versioned documentation system Furthermore, being able to associate any issues with the correct system is valuable for support. We do this by creating a formal release or tag in the version control system (Git or otherwise). This means we can enable bug trackers to associate issues with specific versions.

We will also formulate a Rollback Plan because sometimes even the best organized deployments can fail. If the production environment goes down after a deployment, often the best course of action is rolling back to the previous version of the software. Being able to do so quickly makes all the difference to getting the production environment back up and running — integral to Team DIFZ’s DR approach.

To ensure SOW 5.2.1.3 Facility Safety, Team DIFZ will update existing engineering support SOPs so our staff have clear guidance on managing systems in a safe manner. For example, upon detecting any unauthorized equipment (that is, not provided by NIH or CBITT), we will shut it down if it presents a hazard, is doing harm to, or has harmed the facility. When working on hardware within the Data Center, we will adhere to the NIH or NCI Data Center Infrastructure Guidelines for infrastructure rack, wiring, tools and labeling, and naming standards. Our staff, as part of the onboarding process, will be training in all NIH or NCI Data Center Policy and Work Rules so no behavior strays outside of those requirements.

5.2.2  System Security

DIFZ has provided IT system security-related engineering support to the Centers for Medicare and Medicaid Services (CMS) Information Security and Privacy Groups’ (ISPG) DevSecOps (DSO) Team in compliance with HSPD and FISMA since 2016. As part of ISPG’s DSO Support Team, DIFZ plays a key role in the development of high-value DevSecOps-related solutions that ensure security is “built-in” throughout all phases of each CMS system’s life cycle. Supporting the CMS CISO’s development of DevSecOps approach DIFZ successfully design and demonstrates ISPG’s DevSecOps automation solutions which have assisted with the modernization of the CMS ATO process through automated security compliance testing and documentation through integration of security testing tools into existing CI/CD pipelines. Through automation, the DIFZ DSO solutions team help promote continuous code validation, change, and configuration management.

For any hybrid Agile development, release teams and information assurance experts analyze security data to generate accurate documentation at each Sprint/Release and support faster ATO decisions. The DIFZ Team integrates security baseline hardening and compliance testing into the CI/CD pipeline for cloud applications through development and integration of Chef InSpec Profiles, an open-source framework for testing and auditing applications and infrastructure, into those existing DevSecOps pipelines. Developers maintain agile code delivery, while satisfying compliance requirements and improving internal Security Impact Assessments (SIA). The DIFZ Team also supports development of data protection solutions at rest and in transition that include cost-effective strategies for encryption, secrets management and access control, leveraging existing investments at CMS.

Our teaming partner \_\_\_\_ has experience providing secure data center services — their facilities house the infrastructure that hosts applications used to support the clinical trial process and corporate support functions. These data centers are built to specifications to ensure physical security, hardened to prevent intrusion, and supported by back-up power sources. Their production data center is compliant with HIPAA, Federal Information Security Management Act (FISMA) (High), FedRAMP, ISO 27001, and Payment Card Industry Data Security Standard (PCI DSS) standards. Standardized processes ensure data is backed up. All back-ups are replicated between the two data centers. Only authorized IT staff or facilities staff have data center access. Visitors must be escorted by authorized staff.  We will maintain the SAML Single Sign-on (SSO) federated standard to exchange user identity and authentication information between the CORE systems and other information sources for CTEP Clinical Trials (e.g., NCTN group websites). Team DIFZ will work to expand SSO services for new websites/web-based systems as approved.

There are three essential roles in the government Certification and Accreditation Process (CAP). At a minimum, a system owner, Designated Approving Authority (DAA), and certifying agent are required to implement the process. Team DIFZ has experience at The government with the phases of the C&A process: Initiation, Security Certification, Security Accreditation, and Continuous Monitoring. Each phase consists of a set of defined tasks and subtasks that are to be performed by responsible individuals (e.g.,, system owner, Certifying Agent, user representatives, etc.). Security certification and accreditation activities can be applied to an information system at appropriate phases in the system development life cycle. Additionally, the activities can be tailored to apply a level of effort and rigor that is most suitable for the system undergoing security certification and accreditation. The fundamental purpose of the certification process is to determine if the security controls for the IT system are correctly implemented and are effective in their application. Certification levels establish the level of effort and test methods to be used to verify security controls for security test and evaluation efforts.

The DIFZ Team recognizes that secure physical facilities integrated with strong IT infrastructure, data, and document storage are keys to sensitive data protection, project communications, cost control, and an enhanced user experience. Robust facilities and a computing infrastructure built on best practices and industry-standard hardware and software result in secure and efficient administration of communications, data collection, data management, and storage requirements for hundreds of studies. Information security risk assessments are completed on systems that include relevant responsibilities for review, scope, frequency, risk mitigations actions and approval. SOP IT-04 (Computer Room and Data Security) includes the high-level requirements and process for data backup and recovery.

Security Environment. DIFZ Team operates under standard policies and procedures that provide a framework for information security. We use best security practices as a basis for our information security program and a defense-in-depth strategy to assure confidentiality, integrity, and availability of our sponsors’ sensitive data. Their environment is composed of computers, operating systems, applications and services, networks, operations and monitoring equipment, and specialized hardware, along with the administrative and operations staff required to run and maintain the services. The data centers are also included as part of their security posture; all data center services and physical access have safeguards in place to deter from any malicious or accidental damage. The DIFZ Team chose to adopt the ISO 27001 framework due to the global nature of our provided services, receiving ISO/IEC 27001:2013 certification in 2020 and recertification in 2021.

IT Security Policies and Procedures. The DIFZ Team operates under a standard set of policies, SOPs, Best Practices & Guidelines (BPGs) that provide a framework for our information security environment. The DIFZ Team can provide a full listing of these policies, SOPs, and BPGs during competitive range negotiation responses. We will install software vendor released security patches, update the antivirus definitions to permit automatic updates, and remediate critical and high vulnerabilities in an expedited manner, within agency specified timeframes. Notification of routine updates will occur as part of standard Change Management. We will report any potential security breach in accordance with agency-specific incident response procedures. For example, we will notify the CO, PM, and COR within one-hour, upon realization of any potential security breach.

—

5.2.3 - System Backup and Disaster Recovery Management

Team DIFZ recognizes the difference between backup and disaster recovery, and we understand key concepts that are critical for helloing NCI develop effective strategies. To ensure business continuity, the government needs a robust, tested disaster recovery plan — and an important first activity for our team will be to review the approved Operational Contingency Plan and identify how unusual circumstances might justify deviating as needed in the event of any individual system and component failures. Team DIFZ will audit the plan and processes for quickly reestablishing access to applications, data, and IT resources after an outage. We will assess if the plan should be updated to involve switching over to a redundant set of servers and storage systems until the primary data center is functional again.

We will recommend to the CO/COR how to address any outstanding issues prior to execution of the approved Contingency/Disaster Recovery Plan (C/DRP). Our metric for restoration of CTEP-ESYS critical applications is to get them back up and running within 4 hours, and be fully operational within 24 hours. Part of our preliminary assessment will be to work with the government to set recovery time objectives (RTO) — the amount of time it takes to recover normal business operations after an outage. As we look to set NCI’s RTO, stakeholders will need to consider how much time they are willing to lose — and the impact that time will have on service delivery. We will notify the CO, PM, and COR within one-hour, upon realization of any system failure. The team will work diligently to restore any such failure in the most expedient manner, while providing status updates to the COR as requested by COR post initial synchronous notification until the system failure is resolved.

We will dig deep into the NCI process of making multiple copies of data — the role of back up data is to protect it. We will develop SOPs to restore backup data if the organization encounters an accidental deletion, database corruption, or problem with a software upgrade. We will test these SOPS so we may execute approved C/DRP in the event of a disaster causing shutdown of CTEP-ESYS operations (e.g., catastrophic disaster). If special circumstances warrant, we may suggest deviating as needed, to ensure we can keep NCI’s systems running. Team DIFZ will recommend metrics around a recovery point objective (RPO), the amount of data the government can afford to lose in a disaster. The agency might need to copy data to a remote data center continuously so that an outage will not result in any data loss. Or system owners might decide that losing five minutes or one hour of data would be acceptable. From there, Team DIFZ will document and test the restore process, transferring backup data to the primary system or data center. We consider the restore process as part of backup rather than disaster recovery.

5.3 - TASK 3 - OPERATIONS AND MAINTENANCE

We have in depth experience providing IT operations and maintenance to multiple clients. For example, Digital Infuzion spearheaded the effort at National Center for Advancing Translational Sciences (NCATS) in the areas of CIO support, contract and task order management, project and requirements management, software development, maintenance and operations, customer relationship management, data management and data curation, network, scientific computing, hosting and storage, business process management, information security, bioinformatics and scientific programming, scientific system administration, training, documentation and help desk support. We understand the work to be performed under this task relates to the operation and maintenance of CTEP- ESYS applications and service, but may also entail collaboration with a third-party organization to conduct system audit(s) as needed to verify technical and/or functional components.

Team DIFZ will ensure all CTEP-ESYS applications are fully functional (with the exception of pre-approved scheduled maintenance), 24 hours per day, 7 days per week. For the National Institute of Allergy and Infectious Diseases (NIAID) Clinical Research Management System (CRMS) contract, we support the following key activities: software development, deployment, software maintenance, application integration, business intelligence and analytics, identity and access management, document management, training and documentation, help desk and user support, application security, security assessment and authorization support, data management, data migration, and integration to support key business areas surrounding the NIAID’s research agenda. DIFZ also works with NIAID OCICB to manage the IT infrastructure, which includes database management and storage assessment. Guaranteeing uptime will be a core component of the Service Level Agreement (SLA) metrics we will establish at kick-off. This is an example of how we utilize best practices consistent with our Capability Maturity Model Integration (CMMI) maturity level. As described in our management plan, Team DIFZ utilizes IT Service Management best practices from the ITIL framework to help align IT service delivery with business goals.

As our domain expertise includes HIPAA regulations and compliance; research protocols; application development and enhancement; training; change management; and system security, Team DIFZ implements solutions using a balanced application of our people, processes, technologies, and knowledge assets. This ensures updates are compliant with relevant patient consent provisions of Health Insurance Portability and Accountability Act (HIPAA) as applicable to the CTEP-ESYS. As we did at \_\_\_\_\_\_. our team will maintain compliance with all regulatory requirements concerning patient records in electronic format that are created, modified, maintained, archived, retrieved, or transmitted under agency record requirements. We understand this compliance also applies to any electronic record submitted to the agency. Further, as appropriate, comply with relevant sections of the Code of Federal Regulations (21 CFR Part 11) for computer systems (including hardware and software).

Operations & maintenance extends beyond “keeping the lights on.” For example, other services we will provide include technical and audio-visual support to Government staff for meetings hosted by the Contractor at CTEP facilities. From past experience, our staff are familiar with the audio-visual systems used at NCI Shady Grove campus, having received training from CTEP UC/AV contract located at that facility. We will review that training after award to ensure we can enhance NCI stakeholder customer experience with a “silk glove” approach. Another aspect of this approach is the drafting of a list of critical stakeholders who may need desk side or enhanced support for technical issues. Help desk personnel will know to provide priority service as needed for the most important users.

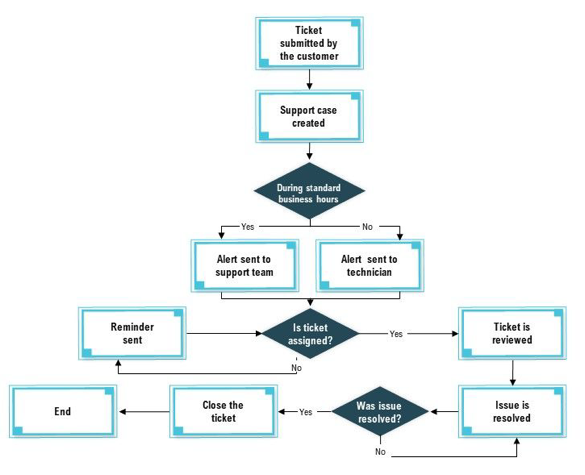
5.3.1 Help Desk

Team DIFZ understands that the key to trouble ticket management is having a process–a good one–and sticking to it. Our ticket response process uses ISO900x standards for quality improvement, and is based on ITIL methodologies. Our approach is to identify an incident coming via our Automated Call Distribution call center, as an email, or via web-based applications. Self-service via the portal and our help desk support system pre-classifies incidents, and automatically logs the ticket. If handled on the telephone by our technicians, the service team’s task is to properly log it in our help desk system. The logging captures the name of the person reporting the incident; date and time the incident is reported; description of the incident, such as what service is down or what device is not working properly; and, a unique identification number, for tracking. Either self-assigned, or by one of our experienced technicians, the incident is categorize and prioritized with custom labels, and sub-categories as appropriate.

Response is made, first via initial diagnosis. If the ticket is processed via the self-service web portal, the end user may be presented with potential solutions drawn from the help desk support system knowledge base. A Team DIFZ help desk technician is automatically alerted to a new ticket, assigned on the technician’s availability and skill set. The DIFZ team member formulates a quick hypothesis around what is likely wrong, so they can either set about fixing it or follow the appropriate procedures and deploy the right resources to get it resolved. This is not unlike the triage function that a hospital emergency room performs on new patients.

Our front-line support team should be able to resolve a large number of the most frequent incidents without escalating. But when required, the assigned technician will gather and log the right information to help second and third-level (more technical) support get up to speed quickly, so they can resolve the incident promptly. While ITIL identifies investigation as a discrete step, at Team DIFZ diagnosis happens throughout the incident lifecycle. Eventually and ideally within our government-agreed upon service level agreement (SLA) – the Team DIFZ support technician will arrive at a diagnosis and perform the necessary steps to resolve the ticket. This recovery is mapped to a metric calculating the amount of time it may take for operations to be fully restored, since some fixes (like bug patches, etc.) may require testing and deployment even after the proper resolution has been identified.

The incident ticket automatically passes back to the help desk (if escalated) for close out. To maintain quality and ensure a smooth process, only Team DIFZ service technicians are allowed to close incidents, and the end user reporting the incident will be automatically notified, to confirm that the resolution is satisfactory. Every closed ticket further builds the knowledge base, and supports our ISO900x quality effort by dispatching an email-based customer satisfaction survey. The survey results drive reporting metrics (delivered in near-real time via an administrative function of the help desk support system). When needed, Team DIFZ personnel will utilize remote access to troubleshoot systems. We will support resolution of access issues, including on boarding new user accounts, password resets, and user access issues. All tickets will be categorized and resolved properly to ensure smooth business operations, as showing in the following exhibit.

**Exhibit x. Ticket Processing**

As we will be supporting CTEP-ESYS end-users, NCI staff and Contractors, Team DIFZ will ensure effective problem identification and resolution. To do so, we categorize user problems based on the type of problem received from both internal and external users. These problem tickets are then assigned to the appropriate personnel for resolution. Our team will monitor the ticket tracking system for tickets that are assigned or transferred to the project. We will resolve tickets by making an initial assessment of the issue presented. We will use our ITIL-based strategy for responding to service desk tickets.

Depending on the ticket category, we will research the problem by looking at log files, error files, inspecting the status of records in the database tables, and by taking other measures as necessary. Once the problem is identified and a solution is found, we will communicate with all affected parties to advise them of any required activities needed from them. If a condition arises where the solution involves action from other parties, we will involve the relevant stakeholders to discuss next steps and establish priorities. Implementation of certain desired solutions will vary depending upon the complexity of the desired fix. For all application releases, we will prepare briefing materials and distribute those among the program area staff to apprise them of the release changes.

**Exhibit x. Ticket Classification**

A key outcome is speedy and thorough resolution of issues, and a high level of end user customer satisfactions. Our value-add is that we enable the front line support team with an organic, self-improving knowledge base populated with articles and incident diagnostic scripts to help them resolve tickets quickly. Because our ITIL methodology calls for the service desk to retain control of incident progress, routing, and status, we deliver continually improving quality. Proof point: At\_\_\_\_\_\_\_, Team DIFZ decreased ticket closure times by \_\_\_, following implementation of our ITIL-based methodologies that standardized logging every incident with a unique ID in the service desk software. In operating the help desk to provide optimal coverage during workdays, Team DIFZ will make sure CTEP-ESYS end-users around the globe will have telephone and email access to help desk staff, including providing after-hours capture of customer support requests (e.g., voice mail, email) so we may support requests regarding all facets of CTEP-ESYS operations.

| **Severity Level** | **Response Time** | **Description** | **Resolution Time** |
| --- | --- | --- | --- |
| Critical | Within 15 minutes | Complete outage, multiple users impacted, no immediate workaround | Within 8 hours |
| High | Within 1 hour | Degraded service, multiple users affected, latency issues, unable to log into systems | Within 12 hours |
| Medium | Within 4 hours | Does not immediately impede mission performance, only one user affected, work arounds exist, break/fix request. We will provide an initial response to all requests within 4 work hours of receipt during working hours. Requests received during after-hours will receive a response within 4 hours of the start of the next working day. | Within 3 business days |
| Low | Within 1 business day | Equipment upgrade, move, new component or enhancement. Impact is low and work can be scheduled based on business case | Within 7 business days |

Team DIFZ’s unique combination of software support tools and proven processes mean we don’t just capture incident data, we analyze it to look for trends, patterns, and potential underlying problems. This ultimately can reduce incident volume and mitigate risk. To do this, we will enhance the help desk triage system to promote rapid and accurate response to queries, and ensure ticket categorization according to service desk best practices (e.g., ITIL) so we can differentiate between an incident (e.g., break/fix) or a service request. Our team will utilize the help desk log to identify targeted areas to improve CTEP-ESYS operations and user experiences and present those to COR for consideration. For example, tick log analysis might detect repetitive “bugs” or defects that impact day to day work for users. We would then submit an appropriate change request to solve that issue, proactively.

At the kick-off meeting, we will work with the CO/COR and CTEP leadership to ensure response timelines are appropriate for the type of assistance requested (e.g., currently CTEP-AERS SAE report submission issues must be addressed within 4 business hours). Based on years of managing help desk solitons, Team DIFZ can bring creative solutions for the help desk functions that enhance relations with CTEP-ESYS clients. These innovations also help to conserve resources at the help desk to avoid excessive staffing requirements (e.g., a “tier 0” portal with Knowledgebase, FAQs, Quick-tips, etc.). We will import develop mechanisms to track customer satisfaction and identify processes that provide additional benefit, using a “lessons learned” approach.

5.3.2 Incidents (Break/Fix Support)

[WRITING IN PROCESS]

5.3.3 Configuration Management (CM)

Information systems that are designed or developed for or on behalf of NIH at non-NIH facilities shall comply with all NIH policies developed in accordance with Federal Information Security Modernization Act (FISMA), NIST, and related NIH security and privacy control requirements for Federal information systems. This includes information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization. The current FIPS 199 categorization is Moderate. The security controls must be designed, developed, approved by NIH, and implemented in accordance with the provisions of NIH security system development life cycle as outlined in NIST Special Publication 800-37.

DIFZ will tailor its Configuration Management (CM) Plan to support NCI systems. The plan will identify the CM organization, management policies and, by specific reference, standard practices and detailed work instructions to be used in implementing the configuration management processes during the implementation of the products during the contract.  Our configuration management system approach will detail in terms of applicable requirements, planned implementation methods, configuration verification methods, schedules, and organizational structure as well as management tools and guidelines for both hardware and software systems as defined in line with CMMI Level 3 processes and practices. Our CM Plan is intended to enhance the overall process efficiency and collaboration between CTEP stakeholders. Our CMMI v2.0 CM processes include configuration identification, change control, status accounting and audits using tools such as SharePoint Server, Azure DevOps and GitHub.

Configuration Identification: DIFZ will encapsulate all items to be included and managed for the life cycle of available systems. This will capture documentation, source code, hardware and software configurations, binary files, and runtime dependencies to be controlled by the gatekeeper.

Change Control: DIFZ will capture and identify all supporting applications and systems and capture and review their corresponding access.  In addition, working with stakeholders establish and maintain list of ownership of each application and system. This function in collaboration with the CTEP Change Control Board shall be used to manage approval from relevant stakeholders on moving changes forward.  Ensuring virus and patch management is current and in accordance with policy.

Status Accounting: DIFZ will capture and report information on the nontechnical status of proposed and pending changes.  The intent of the information is to establish baselines of applications and systems and may be shared with relevant stakeholders and/or COR when an ad-hoc request is received. The information will be primarily derived from the configuration identification list generated.

Configuration Audit: As part of the CM Plan, we will establish a cycle to conduct configuration audits to ensure the established processes are being followed by the DIFZ Team and adjust as necessary. Any non-compliances identified within the planned audits will be reviewed, addressed, and brought to a close using process improvement methods. Furthermore, and more importantly, the intent of this audit is to capture and verify all artifacts to be delivered were indeed delivered to the target system during each intended release.

[WRITING IN PROCESS]

These processes will assist NCI to deploy and align configuration management best practices and improve operational efficiency, enhance productivity, and deliver products and services in the support of its systems, offering measurable business value.

5.3.4 - System Manuals and Training

DIFZ will maintain a set of up-to-date Administrator/System manuals detailing the operational procedures and business rules for all CTEP-ESYS applications. These manuals will be reviewed and approved by the COR prior to posting. Following the same principles as our support for software documentation, DIFZ will maintain and update system documentation in both electronic and hardcopy format for government-developed software systems and COTS software systems. Our technical writers will provide the administrators, developers, and end user documentation to improve understanding on how to implement the functionality of systems. DIFZ technical writers bring the benefit of superior system documentation by preserving the history of the systems at different cycles, thus facilitating the use of it by the users and administrators. We have found an important objective of documentation is to teach those unfamiliar with the system, how it is structured, how it works, and what are the design/use parameters. DIFZ’s approach means documentation can be applied without affecting end user processes, providing a guide. Think of DIFZ’s documentation outputs as the map and compass to navigate complex systems. The updated set of manuals will be posted online to a secure reading room. Administrator/System manuals should be updated as needed with revised versions posted for review and use by project leadership team. All user guides will be submitted to the COR or designee for review prior to posting, and will be updated as needed and/or as requested.

Team DIFZ is experienced at coordinating and delivering training programs for new programs and updating them from existing training materials. We are prepared to augment a training program at with any level of rigor desired by the client. We are well versed in the disciplines of adult learning theory and principles and instructional systems design and implementation. Team DIFZ is experienced in maintenance and development of existing training systems including distance learning, web-based, podium (classroom) based, and stand-alone computer based systems and Learning Management Systems (LMSs). We are familiar with the many commercial off the shelf and custom built Learning Management Systems. We have experience interfacing with and building Sharable Content Object Reference Model (SCORM) compliant systems for web-based training and will assist NCI with adaptation of a SCORM compliant LMS for remote training courses.

Team DIFZ is capable of developing entire training programs, beginning with the development of a Training Plan. To develop the plan, we will use instructional design principles, starting with learning objectives and carrying it all the way through to deployment of the training. We will update and adapt existing training to work best with the Distributed Learning (DL) model. We will use this model to maintain a set of up-to-date user guides for all CTEP-ESYS applications; such user guides will be maintained on the appropriate applications landing page after log in.

3. Develop, update, maintain, and provide training and education materials for all applications (e.g., integrations, enhancements) and provide training to Government and other stakeholder personnel at the direction of the COR. Upon request by the COR, education and training materials must be provided in a format compatible with the CLASS Learning Management System.

Using Microsoft Project, our PM will work with the task lead to ensure tracking of resources and schedules, keep lines of communication open with ad hoc and schedule communications (meetings, telephone and email communiqué, and status reporting). As discussed elsewhere, the DIFZ Team will develop and support enhanced communication regarding CTEP-ESYS activities with stakeholders through our communications plan — which we will incorporate into our PMP, and will delineate the use of monthly project review meetings, release notes, trainings sessions, and presentations.

5.3.5 - IT Planning, Reports and Data Calls

[WRITING IN PROCESS]

5.4 - TASK 4

[INSERT CONTENT FROM SUBS]

**Task 4 / 3.1.2.4.3 - 508 Compliance Requirements [SOW 5.4.3]**

DIFZ will comply with Section 508 standards that provide equal access and use of Electronic and Information Technology (EIT) for people with disabilities (vision, hearing, speech, communication, and fine motor control) for work products delivered through the contract. In addition to the Section 508 Functional Performance Criteria (1194.31), we will adhere to (1) Software applications and operating systems (1194.21); (2) Web-based intranet and Internet information and applications (1194.22); and (3) Information, Documentation, and Support (1194.41).

We will leverage the DIFZ Team’s Section 508 SMEs who have worked on relevant programs at NCI and NIH to help ensure compliance with all Section 508 requirements under this contract. We e provide Section 508 subject-matter expertise and document assessment (e.g., EIT Accessibility Plan, Functional Requirement Documents, Requirement Traceability Metrics, and Voluntary Product Accessibility Template (VPAT)). Our 508 SMEs conduct Section 508 testing using approved Agency tools (e.g., Wave, Sortsite, AccVerify, CommonLook, JAWS, WAT, Object Inspector) to verify compliance with Section 508 standards and Agency Office of Assistive Systems & Technologies (OAST) policies.

To ensure the requirements of 1194.21, 1194.22, and the Agency’s Standards, policies and procedures (Section 508) are met for software applications, operating systems, web-based applications, and Intranet information and applications, we will conduct Section 508 testing as required using the test tools and methods identified by stakeholders. In accordance with 1194.41, we will ensure, upon request, that product support documentation, including documentation describing accessibility and compatibility, is made available in alternate formats and that support services accommodate communication needs of end-users with disabilities. We will ensure that a Section 508 Market Research Document is completed prior to purchase of commercial-off-the-shelf (COTS) applications, data, or services, and we will use a VPAT to document Section 508 compliance of the product.

For all CTEP deliverable products we produce that are subject to Section 508 requirements, we provide a completed Section 508 VPAT, which states exactly how the products meet or do not meet the applicable standards.

DIFZ has proven experience developing and testing systems that are fully compliant with the following applicable Section 508 Standards: Section 1194.21 Software Applications and Operating Systems, Section 1194.22 Web-based Internet Information and Applications, Section 1194.24 Video and Multimedia Products, Section 1194.26 Desktop and Portable Computers, Section 1194.31 Functional Performance Criteria, and Section 1194.41 Information, Documentation, and Support. We build Section 508 compliance into our software from the beginning, testing throughout, instead of adding it late in the development cycle. We will perform 508 compliance analysis. In the planning process for any project, we seek to understand the following items as quickly as possible:

* + Which accessibility standards have been identified for the product
  + If the subject federal agency has noted any exceptions
  + The out-of-the-box capabilities and limits of underlying operating systems and COTS products
  + If there are any special considerations unique to product development

The DIFZ team will ensure that deliverables are compliant with 508 standards and HHS standards and policies, by testing web pages and digital media for compliance, and by remediating existing web pages, EIT, and other materials as needed. As requested, we will go beyond project-centric 508 and provide accessibility services to make specific content available for special needs users, in accordance with 508 Accommodations Guidance. Key components of DIFZ’s 508 Compliance Plan include:

Program Coordination: The 508 Compliance Plan will identify key stakeholders and a 508 Compliance Coordinator, who will work with the NIH 508 Coordinator. For each deliverable, we will identify a Section 508 Point of Contact to oversee compliance during EIT development. Stakeholders will include both NIH personnel and the DIFZ managers and staff members. The 508 Compliance Plan will outline how communication occurs among and between the team and the customer including the provision of a VPAT.

Planning: In the planning stages for each Task Order, the 508 Compliance Coordinator will ensure the work plans, Statements of Work (SOW), schedule(s), and other relevant documents, identify applicable EIT standards and checklists to be used for procurement/development, and include steps for testing and assessment of all EITs as part of an Action Plan.

Risks and Risk Mitigation: A Risk Mitigation Plan will be developed and maintained by the 508 Compliance Coordinator, identifying strategies to mitigate risk.

Metrics and Reporting: The 508 Compliance Plan will identify metrics to demonstrate the effectiveness of our Section 508 implementation. Routine reports will be provided documenting the 508 compliance activities and any areas for improvement. Potential metrics in the report include:

* + Elimination and/or reduction in the number of accessibility complaints filed
  + Project personnel with current Section 508 training
  + Use and accuracy of automated tools used to ensure 508 Compliance
  + 508 Compliant EITs tested and deployed
  + Action plans, audit results, and a risk mitigation plan

Training: DIFZ’s Section 508 Training Program is intended to increase the awareness, understanding, and application of Section 508 standards. We will leverage and supplement materials and resources from HHS and the Federal Government (http://www.hhs.gov/web/508 and www.Section508.Gov) with DIFZ and NIH 508 Coordinator training materials and resources as necessary. As updated materials and information become available, they will be incorporated as well. All project personnel will be required to review training programs upon hire and periodically undergo refresher training.

Implementation: The DIFZ Section 508 POC will monitor the Action Plan for development activities to ensure that the standards are implemented.

Testing and Assessment: All EIT deliverables under this contract will go through a 508 Compliance Test before being released into production. We have experienced testers who use tools such as JAWS and NVDA to verify page navigation, logical order of the content, etc. We will also test pages for tab navigation, validate alternate text of images to make sure they convey accurate descriptions of the images and make sure accessibility keyboard shortcuts are not affected. We will continue to test using browser-based WAVE tool for color contrast, html hierarchy, inspect page structure and outline view for readability when styles are disabled and table headings. Our developers also use automatic scanning tools such as PowerMapper SortSite to scan the entire website and work on remedy. Using the HHS 508 compliance form as the baseline, conformance criteria specific to each type of technical component will be used to test for, and ensure, overall product conformance to 508 performance standards. We will modify any EIT deliverables that do not comply with minimum 508 Compliance standards. Reports will be maintained by the Technical Lead and provided to the NIH 508 Coordinator.

Some Commercial-Off-The-Shelf (COTS) software products may have limitations or only be partially compliant with Section 508. In this case, DIFZ will follow the process for exceptions outlined in the 508 Compliance Plan. The process, as understood, is to submit a waiver request through the NIH 508 Coordinator for approval and forwarding to the Information Security Systems Officer (ISSO). Standard waiver reasons as defined by the NIH 508 Coordinator will be used and status of the waiver request will be tracked and monitored.

The 508 Compliance Form, VPATs, Waivers, and other critical documents will be archived for reference and traceability for each EIT assessed in a database/repository location defined with the NIH 508 Coordinator and Executive Sponsor. DIFZ will fully support the successful implementation of the Section 508 Compliance Plan to ensure that all EIT deliverables will provide access to information, programs and services of NIH and improve accessibility and opportunity for those with disabilities.

DIFZ will make every effort to implement every subpart of Sections 1194.21 and 1194.22 as well as abide by Section 508 compliance for all reports and deliverables that are generated through this Task Order. The VPAT will be delivered and provide information on how the work products developed in the context of this SOW will be maintained to conform to Section 508 Accessibility Standards.

For other electronic deliverables such as electronic documents and reports, we ensure they are made 508 Compliant for print disabled participants to include colored and textured objects, and formatting material to be read by a screen reader (Alternative Text). All diagrams are saved as objects, and Alt Text added for each diagram. The person needing this view can always refer to this source during and after meetings. Screen reader software (assistive technology used as a reasonable accommodation) is available (but not provided by the contractor), that will read the Alt Text aloud for each diagram and navigate the document in logical order. Graphics using color to convey meaning have been updated to use a color-blind acceptable color palette. Shades of orange, grey and blue, as well as textured objects have replaced traditional color schemes. As an additional accommodation to print disabled meeting participants, all material presented on each diagram is read aloud during a meeting.