



Service Definition Document

TTEC Digital NiCE IEX Workforce Management
(WFM)



Table of Contents

Table of Contents	2
1. Introduction	4
1.1. Company Overview	4
1.2. Value Proposition.....	6
1.3. What the Service Provides	7
1.4. Overview of the G-Cloud Service	8
1.5. Associated Services.....	9
2. Data Protection	12
2.1. Information Assurance/Security.....	12
2.2. Back-Up and Restore	14
2.3. Data Processing and Storage Location	16
2.4. Data Restoration / Service Migration	18
2.5. Business Continuity Statement / Plan.....	19
2.6. Privacy by Design	22
3. Using The Service.....	23
3.1. Ordering and Invoicing Process.....	23
3.2. Availability of Trial Service	23
3.3. On-Boarding	24
3.4. API	26
3.5. International SMS.....	28
3.6. Off-Boarding	30



3.7. Training	31
3.8. Implementation Plan	33
3.9. Service Management	36
3.10. Service Constraints	37
3.11. Service Levels	39
3.12. Outage and Maintenance Management	41
3.13. Financial Recompense Model for not Meeting Service Levels..	44
4. Provision of the Service	45
4.1. Customer Responsibilities	45
4.2. Technical Requirements and Client-Side Requirements	45
4.3. Browsers	45
4.4. Outcomes/Deliverables	46
4.5. Development Life Cycle of the Solution	46
4.6. After Sales Account Management	46
4.7. Termination Process	47
5. Other Messaging Services	48
6. Environmental Action and Social Value	49
6.1. Environmental Action	49
6.2. Social Value	50
7. Our Experience	52
7.1. Case Study	52



1. Introduction

1.1. Company Overview

G-Cloud 15 Legal Entity and Ownership

TTEC Consulting (UK) Limited, a TTEC Digital Company, is the legal entity for G-Cloud 15. TTEC Consulting (UK) Limited is ultimately owned by TTEC Holdings, Inc., a listed company publicly traded on the NASDAQ Stock Exchange.

Parent Company Overview: TTEC Holdings, Inc.

TTEC Holdings, Inc. (NASDAQ:TTEC) is a leading global customer experience (CX) technology and services innovator for AI-enabled digital CX solutions. Serving iconic and disruptive brands, TTEC's outcome-based solutions span the entire enterprise, touch every virtual interaction channel, and improve each step of the customer journey.

TTEC operates through two business segments:

- TTEC Digital: Designs, builds, and operates omnichannel contact centre technology, CRM, AI and analytics solutions.
- TTEC Engage: Delivers AI-enabled customer engagement, customer acquisition and growth, tech support, back office, and fraud prevention services.

TTEC Digital: Customer Experience Technology and Consulting Services

At TTEC Digital, we offer customer experience (CX) consulting, software, and technology services at the intersection of contact centre, CRM, AI and analytics. We call this intersection the point of conversation and we apply our expertise here to drive shareholder value for our clients in the form of revenue growth, cost reduction, and productivity improvement.

In today's digital landscape, customer conversations and the contact centre technologies that support them are inseparable. With decades of innovation across leading contact centre



platforms and deep expertise in CX strategy, data, and AI, TTEC Digital enables organisations to maximise their technology investments and create exceptional customer experiences.

TTEC Digital: Strategic Partnerships

TTEC Digital leverages a robust ecosystem of strategic alliances to deliver world-class customer experience solutions. As a Genesys Global Platinum Partner, we design and deploy advanced cloud contact centre platforms that drive operational efficiency and customer engagement. Our integrations extend across leading technology providers, including NiCE for workforce optimisation, Microsoft for collaboration and CRM through Dynamics 365 and Teams, and Google Cloud for AI-driven conversational experiences. We partner with Cisco to enable secure, scalable network and telephony solutions, and with ServiceNow to unify service workflows and agent desktops. Our Salesforce expertise ensures seamless omnichannel CRM orchestration, while AWS powers intelligent automation and secure cloud infrastructure. Additionally, our collaboration with Pega supports dynamic case management and process automation. These partnerships enable TTEC Digital to deliver innovative, scalable, and secure solutions tailored to the evolving needs of public sector organisations.

- Microsoft: Seamless CRM and productivity integration through Dynamics 365 and Teams.
- Genesys: Global Platinum Partner delivering advanced cloud contact centre solutions.
- NiCE: Workforce optimisation and analytics for operational excellence.
- ServiceNow: Unified service workflows and agent desktop integration.
- Google Cloud: AI-driven conversational experiences and scalable infrastructure.
- Cisco: Secure, scalable network and telephony solutions for enterprise-grade CX.
- Salesforce: Omnichannel CRM orchestration and customer engagement expertise.
- AWS: Cloud infrastructure and services for scalability and innovation.
- Calabrio: Advanced workforce engagement and analytics solutions.
- Shelf: Knowledge management platform for streamlined agent support and efficiency.



1.2. Value Proposition

TTEC Digital enables G-Cloud organisations to provide secure, citizen-focused, and digitally advanced services through a broad suite of capabilities. Our methodology integrates consulting proficiency, sophisticated technology platforms, and managed services to achieve quantifiable results and maintain compliance with UK standards.

Core Pillars of Our Value Proposition

- Customer-Centric Solutions
 - Our approach is centred on the needs of citizens and end users, ensuring that every service is designed to deliver a seamless and positive experience. We tailor our solutions to address specific organisational goals while maintaining a strong focus on accessibility, ease of use, and satisfaction at every interaction.
- Digital Transformation Expertise
 - Drawing on deep knowledge and experience in digital transformation, we guide organisations through every stage of technological change. Our team ensures that the adoption of new platforms, tools, and processes is smooth, effective, and aligned with long-term business objectives.
- Integrated Multichannel Engagement
 - We enable organisations to interact with citizens and customers across a range of channels, including voice, digital, and self-service options. This integrated approach ensures that people can engage in the way that suits them best, resulting in more meaningful and effective communication.
- Data-Driven Insights
 - Our solutions leverage advanced analytics and data to provide actionable insights. By turning data into knowledge, organisations can make informed decisions that drive continuous improvement and deliver measurable outcomes for both stakeholders and citizens.
- End-to-End Delivery



- We manage the complete lifecycle of each engagement, from initial consultation and solution design through to implementation and ongoing support. This comprehensive approach ensures consistency, quality, and reliability at every stage of the project.

1.3. What the Service Provides

Empowering Contact Centres for Exceptional Customer Experience

TTEC Digital's NICE IEX Workforce Management solution transforms contact centres into strategic engines for customer experience (CX). Designed for flexibility, scalability, and compliance, this cloud-based platform enables organisations to optimise workforce operations while delivering superior service.

Key Benefits

- Market-Leading CX: Omnichannel engagement with a 360° customer view for seamless interactions.
- Local & Compliant: Fully aligned with UK GDPR, Cyber Essentials, and GDS Service Standards for secure, regulatory-compliant operations.
- Work Anywhere: Cloud-first architecture supports home, remote, and hybrid work models.
- Scalable & Flexible: Adapt to changing workforce sizes, locations, and models with ease.
- Evergreen Innovation: Continuous feature upgrades for faster go-to-market and future-ready capabilities.
- Cost Efficiency: Reduce annual charges with pay-per-use pricing and optimised resource allocation.

Core Capabilities

- AI-Powered Forecasting & Scheduling: Predict demand accurately and optimise staffing for peak efficiency.
- Agent Self-Service Portal: Empower agents with visibility and flexibility in managing schedules.



- Omnichannel Workforce Management: Manage voice, email, chat, and social channels seamlessly.
- Performance & Engagement Tools: Drive quality assurance, coaching, and employee engagement.

Why TTEC Digital?

- Deep CX Expertise: Decades of experience in transforming contact centres into growth engines.
- Strategic Partnerships: Collaboration with NICE and leading platforms ensures best-in-class technology.
- End-to-End Services: From consulting and integration to managed services and 24/7 support.

Compliance & Security

- UK Government Cloud Security Principles
- GDPR-compliant data handling
- ISO-certified processes for resilience and protection

1.4. Overview of the G-Cloud Service

NiCE IEX WFM is an intelligent, user-friendly platform designed to help government contact centres deliver efficient, reliable, and citizen-focused services. It enables workforce management leaders to make informed decisions that address both immediate operational needs and long-term strategic objectives.

Key Capabilities for Public Sector Contact Centres

- Accurate Forecasting and Scheduling
 - Harness AI-driven forecasting to predict demand across multiple channels and optimise staffing levels. This ensures the right resources are available to meet



citizen needs without unnecessary overstaffing, supporting cost efficiency and service quality.

- Empowering Agents
 - Through a secure self-service portal, agents can view schedules, request leave, swap shifts, and monitor performance. This transparency and flexibility foster engagement and morale, helping retain skilled staff in a competitive labour market.
- Multi-Channel Service Management
 - Manage forecasting and scheduling for phone, email, web chat, and other channels in one unified system. This is essential for government organisations delivering services through diverse communication methods.
- Real-Time Operational Control
 - Intraday management tools provide supervisors with live visibility into adherence and performance. This enables rapid adjustments to staffing and schedules to handle unexpected fluctuations in demand, ensuring continuity of service.
- Seamless Data Integration
 - Smart Sync technology integrates IEX WFM with other contact centre systems, reducing duplication and streamlining workflows. This supports compliance, data accuracy, and operational efficiency across government environments.

1.5. Associated Services

These optional add-ons extend the functionality of NiCE IEX Workforce Management (WFM) to meet complex operational requirements within UK Government contact centres. They are available as part of the G-Cloud framework and can be procured alongside the core WFM solution.



1. Enhanced Strategic Planner (ESP)

Description:

Provides advanced capacity planning and scenario modelling capabilities for long-term workforce strategies. ESP enables government organisations to forecast resource needs months or years ahead, supporting budget planning and service continuity.

Benefits:

- Long-term demand modelling for multi-channel environments.
- Scenario analysis for policy changes or seasonal peaks.
- Supports compliance with workforce planning standards.

2. Employee Engagement Manager (EEM)

Description:

Automates intraday staffing adjustments and empowers agents with real-time self-service tools. EEM improves flexibility and responsiveness to fluctuating citizen demand.

Benefits:

- Dynamic schedule optimisation during live operations.
- Agent-driven shift swaps and time-off requests.
- Enhances morale and reduces attrition.

3. Additional Integrations

Description:

Expand connectivity beyond the initial ACD integration to include HR systems, LDAP, and other enterprise applications. Optional weekend cutovers and lab/stage environments are available for testing and resilience.

Benefits:

- Seamless data flow across government systems.



- Reduced manual intervention and improved accuracy.
- Supports secure identity management and compliance.

4. Professional Services

Description:

Expert consultancy and configuration services to maximise the value of NiCE IEX WFM. Includes workshops, custom export setup, and Customer Experience Transformation (CXT).

Benefits:

- Tailored solution design aligned to government objectives.
- Accelerated adoption and ROI.
- Ongoing optimisation for efficiency and citizen service.

5. Managed Support Services

Description:

Comprehensive support framework including 24/7 technical assistance, SLA monitoring, and proactive system health checks.

Benefits:

- Guaranteed response times for critical incidents.
- Continuous service improvement.
- Compliance with government service standards.



2. Data Protection

2.1. Information Assurance/Security

Information security is one of the important pillars of TTEC Holdings, Inc. (NASDAQ: TTEC) and TTEC affiliates core global business model, and maintaining it is crucial for our company, our stakeholders, and our clients. By performing internal audits and independent IT compliance audits, the results provide information that can be used to improve operations, enhance accountability, and identify areas for improvement.

The adherence and certification to multiple compliance frameworks ensures that TTEC maintains industry standards to secure data and network systems for our business and our clients. To maintain compliance across these frameworks, TTEC contracts an independent, third party, accredited, qualified auditing firm to conduct the following assessments. Depending on the platform, TTEC technology environment and business facility space, TTEC aligns and is certified under these compliance frameworks:

Engage:

- PCI DSS (Service Level 1) - maintained and assessed annually.
- SOC 1 Type II (SSAE 18) - maintained and assessed annually.
- SOC 2 Type II (SSAE 18 / 4 of the 5 Trust Principles) - maintained and assessed annually.
- ISO 27001: 2022 - maintained and assessed annually. Full assessment year 1, surveillance audits year 2 and 3.
- HIPAA S.C.R.A. - maintained and assessed annually.

Digital:

- PCI DSS (Service Level 1) - maintained and assessed annually.
- SOC 2 Type II (SSAE 18 / 4 of the 5 Trust Principles) - maintained and assessed annually.



- ISO 27001: 2022 - maintained and assessed annually. Full assessment year 1, surveillance audits year 2 and 3.
- HIPAA S.C.R.A. - maintained and assessed annually.

TTEC Consulting (UK) Limited and TTEC (UK) Solutions Limited Environments (EU Cloud Services Only):

- Cyber Essentials Certificate of Assurance (Basic) - maintained and assessed annually for EU cloud services only.
- Cyber Essentials Certificate of Assurance (Plus) - maintained and assessed annually for EU cloud services only.

Cyber Essentials and Cyber Essentials Plus are certifications developed and recognised by the UK government to help organisations protect themselves against common cyber threats and demonstrate their commitment to cybersecurity best practices.

TTEC's achievement of the Cyber Essentials and Cyber Essentials Plus certifications validates TTEC's security controls and safeguards implemented and maintained adhere to these cybersecurity best practices, how we secure TTEC and our clients against common cyber threats and how TTEC demonstrates, annually, our commitment to improving our cybersecurity posture to align to these best practices.

The following provides an overview of each Cyber Essentials Certification assessment which includes but not limited to:

- Cyber Essentials Certification:
 - Focuses on five key areas of cybersecurity: boundary firewalls and internet gateways, secure configuration, user access control, malware protection, and patch management.
 - Designed for organisations of all sizes and sectors.



- Requires organisations to complete a self-assessment questionnaire and provide evidence of their cybersecurity measures.
 - Certification is valid for one year and can be renewed annually.
 - Provides a basic level of assurance to customers, suppliers, and stakeholders that an organisation has implemented essential cybersecurity controls.
- Cyber Essentials Plus Certification:
 - Includes all the requirements of Cyber Essentials certification.
 - Involves an independent assessment and verification of an organisation's systems to ensure they meet the necessary security standards.
 - Requires organisations to undergo vulnerability scanning and penetration testing.
 - Provides a higher level of assurance compared to Cyber Essentials certification.
 - Certification is valid for one year and can be renewed annually.

2.2. Back-Up and Restore

Backup and restore processes in NiCE IEX WFM ensure data integrity, business continuity, and disaster recovery for contact centre operations. These processes protect critical workforce management data such as schedules, forecasts, adherence metrics, and configuration settings.

Backup Strategy

- Regular Database Backups
 - NiCE IEX WFM environments typically perform full and incremental backups of all system databases. These backups include configuration data, historical performance records, and agent schedules.
- Geographically Redundant Storage
 - Backups are replicated across carrier-grade data centres and AWS cloud services in multiple regions (e.g., Europe, North America) to ensure survivability in case of a localised outage.



- Automated Export Modules
 - For NiCE IEX WFM Integrated, 21 export modules allow scheduled data extraction for external storage or analytics. These exports can be configured for cadence (daily or weekly) and retention (typically 7 days on SFTP before removal).
- Security Controls
 - Backup files are encrypted in transit and at rest, complying with GDPR and ISO standards. Access is restricted to authorised administrators only.

Restore Process

- Disaster Recovery Framework
 - NiCE maintains a Resiliency Event Management Plan (REMP), which defines escalation paths and recovery steps. In case of failure, systems can be restored from the latest backup without data loss. This aligns with stringent "Recovery Point Objective (RPO)" meaning the data loss window is zero, a standard for mission-critical WFM data.
- Failover and High Availability
 - NiCE CXone and IEX WFM leverage active-active network topology and transparent failover, ensuring minimal disruption during restore operations.
- Testing and Validation
 - Quarterly failover drills and annual disaster recovery tests validate restore procedures and confirm operational continuity.

Best Practices

- Schedule daily backups for critical data and weekly full backups.
- Use export modules for additional redundancy and reporting needs.
- Regularly review and update disaster recovery documentation.
- Conduct restore drills to ensure readiness for real-world incidents.

Why It Matters for UK Government



Robust backup and restore capabilities are essential for:

- Compliance with UK Government Cloud Security Principles and GDPR.
- Operational Resilience during emergencies or cyber incidents.
- Data Integrity for citizen service continuity.

2.3. Data Processing and Storage Location

NiCE IEX Workforce Management (WFM) is delivered as a cloud-based solution. This section outlines how data is processed, stored, and secured in compliance with UK Government requirements and G-Cloud standards.

Data Processing

- Minimal Personal Data Handling
 - NiCE IEX WFM does not process personal data as part of its core functionality for Named Licenses. Any personal data processed is limited to support requests initiated by the customer and handled under strict GDPR-compliant protocols.
- Role of NiCE
 - NiCE acts as a data processor under customer instructions. All processing activities adhere to UK GDPR and EU GDPR principles, including lawful basis, minimisation, and encryption.
- Security Controls
 - Data in transit is encrypted using TLS 1.2 or higher.
 - Data at rest is encrypted using AES-256.
 - Access is restricted to authorised personnel only, with multi-factor authentication.

Data Storage Location

- Primary Hosting Regions
 - NiCE IEX WFM operates on carrier-grade, geographically redundant data centres and AWS cloud infrastructure.



- Approved hosting locations include:
 - United Kingdom
 - European Union
 - United States
 - India
 - Philippines
- These locations are governed by contractual safeguards, including Standard Contractual Clauses and UK Addendum for restricted transfers.
- **Redundancy & Resilience**
 - Active-active architecture ensures 99.99% uptime.
 - Data replication across multiple regions for disaster recovery.
 - Quarterly failover drills and annual disaster recovery tests validate resilience.

Compliance & Certifications

- Fully aligned with UK Government Cloud Security Principles.
- GDPR-compliant data handling and international transfer safeguards.
- ISO 27001, SOC 2, and penetration testing frameworks in place.

Backup & Restore

- Daily incremental and weekly full backups of system databases.
- Backups encrypted and stored in geographically redundant locations.
- Restore processes validated through regular disaster recovery drills.

Customer Responsibilities

- Ensure appropriate user access controls within the NiCE IEX WFM environment.
- Notify NiCE of any specific UK data residency requirements prior to deployment.

**Benefits for UK Government**

- Data Sovereignty: UK and EU hosting options available.
- Operational Continuity: High availability and disaster recovery built-in.
- Compliance Assurance: Meets G-Cloud and UK GDPR standards.

2.4. Data Restoration / Service Migration

Ensuring business continuity and compliance for UK Government contact centres.

Data Restoration

- Secure Backups: Daily incremental and weekly full backups of schedules, forecasts, and configurations. Encrypted and stored in geographically redundant locations.
- Disaster Recovery: NiCE's Resiliency Event Management Plan (REMP) with quarterly failover drills and annual recovery tests aligned to UK Government Cloud Security Principles.
- Restore Process: Rapid recovery from validated backups, including database restoration, ACD reconnections, and environment validation before resuming operations.

Service Migration

- Scenarios:
 - Cloud-to-cloud migration to NiCE CXone.
 - ACD integration changes (e.g., Genesys, Avaya).
 - Version upgrades with minimal disruption.
- Steps:
 - Assessment & planning of dependencies.
 - Data export via SmartSync and integrity validation.
 - New environment build and secure configuration.
 - Testing, cutover during low-impact windows, and post-migration Hypercare.



- Professional Services: Project governance, technical setup, training, and change management delivered by NiCE and partners like TTEC Digital.

Compliance & Security

- UK GDPR, ISO 27001, SOC2, and UK Government Cloud Security Principles.

Benefits

- Operational Continuity: Rapid recovery and seamless migration.
- Data Integrity: Secure handling of workforce data.
- Future-Ready: Cloud scalability and compliance with digital transformation goals.

2.5. Business Continuity Statement / Plan

TTEC and TTEC's affiliates are committed to business continuity planning, a prudent business practice to protect employees, clients, stakeholders, and TTEC from various risks and events that may impact the ability to conduct business. TTEC's programme aligns with ISO 22301, NIST 800-34 & 84, CSF (Cyber Security Framework) and Disaster Recovery Institute International – The Professional Practices for Business Continuity Management.

TTEC, being a global company, must remain diligent and be prepared when unexpected incidents occur (fire, earthquakes, typhoons, hurricanes, human events, etc.). TTEC's Crisis and Resiliency Management programme, which includes Business Continuity (BC) and IT Disaster Recovery (DR), emphasises the ability to continue providing business services in the face of adverse operational impacts. TTEC's Global Crisis Management Programme is led by the Vice President of Business Continuity (BC) and IT Disaster Recovery (DR).

TTEC's approach to global crisis and business continuity and IT disaster recovery is to adhere to guiding principles of: Putting People First; Establish Trust; Protection of Clients; and Providing Leadership, with managing unexpected and expected incidents and events. With a strong focus



on these principles, TTEC will have the ability to anticipate, prevent, recover from, and learn from crises that may impact employees, facilities, brand/reputation, or operations. Along with TTEC achieving the protection of TTEC's people, TTEC's clients and client's brand, profits and TTEC's brand.

TTEC's Global Crisis and Business Continuity (BC) and IT Disaster Recovery (DR) Management programme has developed a product-driven customer focused recovery model that is both practical and scalable. TTEC establishes, implements, and maintains world class crisis response capabilities through solidifying policies and procedures for response to an emergency or other occurrence that can compromise the privacy, confidentiality, integrity, or availability of Client Personal Information and/or damage TTEC's information systems. Such policies and procedures include, but are not limited to: creating and maintaining retrievable copies of Client Personal Data; restoring any loss of Client Personal Information; enabling continuation of critical business processes involving Client Personal Information in emergency mode; assessing relative criticality of specific applications and Client Personal Information to support other contingency plan components; periodic and annual testing and updates of contingency plans and implement lessons learned from testing.

The programme integrates and builds upon existing capabilities within our Security Event Handling Plan, Information Security Operations, Business Continuity, IT Disaster Recovery and Virtual Response teams. Additional partners in resiliency include Information Technology, Operations, Real Estate and Facilities, Legal, People and Culture, and other shared services. The unifying approach and framework are contained in TTEC's Global Crisis Management Policy for managing and responding to crises across TTEC's global enterprise (including but not limited to WFH environment).

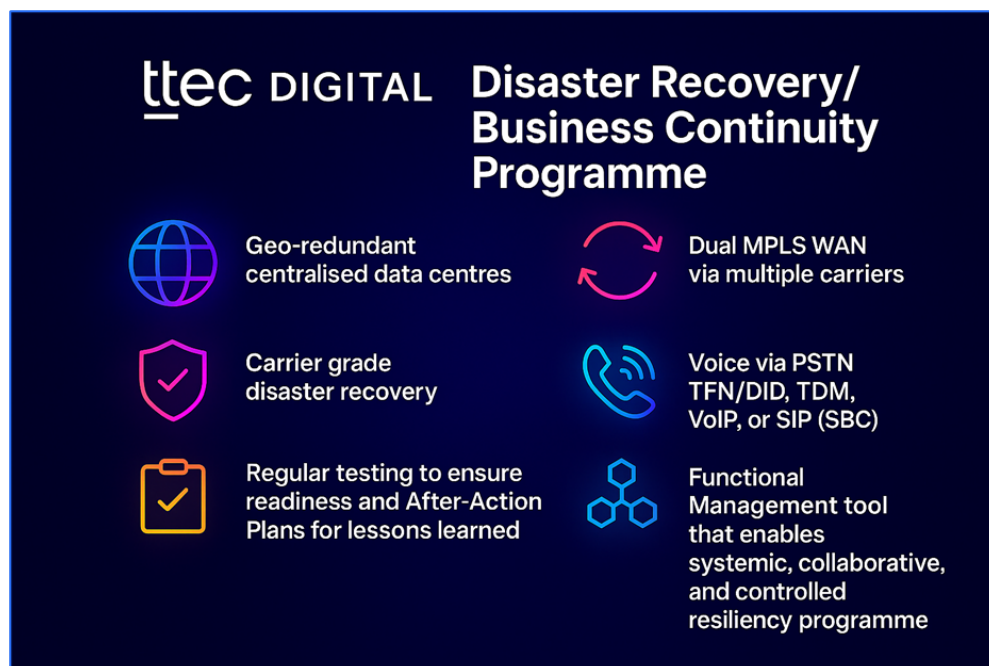
TTEC provides redundancy in our technology through hardware and software configuration. Redundancy provides clients with the services that in the event of hardware failure, or software failure, services remain active and available.



Redundant premise equipment mitigates the risk of equipment failure; dual firewalls with stateful inspection, dual routers, and dual core switches in the data centre provide a highly available architecture for client links. TTEC firewall infrastructure provides stateful inspection and the configuration is in active/active or active/standby mode depending on the project specifications/requirement.

The different types of DRP technology and redundancy capabilities used include but not limited to:

- Geo-redundant centralised data centres.
- Dual MPLS WAN via multiple carriers.
- Carrier grade disaster recovery.
- Voice via PSTN TFN/DID, TDM, VoIP, or SIP (SBC).
- Regular testing to ensure readiness and After-Action Plans for lessons learned.
- Functional Management tool that enables systemic, collaborative, and controlled resiliency programme management.





In addition, at least annually, TTEC's Executives (Sr. Advisor BCDR/Resiliency, CSO, CIO, IT, and other supporting departments) review the Global Crisis Programme and the Business Continuity and IT Disaster Recovery plans, processes, and policies, update (as needed) to align to TTEC's business, security and compliance models and adherence with industry compliance framework requirements. TTEC's BCDR and applications are exercised annually and are governed by our Crisis Management and Disaster Recovery policies and guidelines. TTEC's Global Crisis and Resiliency Management Programme, including TTEC's Security Event Handling Programme is assessed and maintained annually, and is certified against TTEC's ongoing industry compliance audit assessments of PCI DSS, SOC 2 Type II, ISO 27001:2022, HITRUST and more.

Lastly, regarding TTEC's Business Continuity (BC) and IT Disaster Recovery (DR) plan approach, TTEC bridges a partnership with our clients with the development of a specific client focused business continuity (BC) and disaster recovery (DR) plans. TTEC collaborates with clients to build a tailored, resilient, and mutually agreeable BC and IT DR plan that encompass applicable TTEC Technology and Services, prevailing industry compliance standards, information security controls, safeguards, and measures, along with operational best practices, and client-specific SLA requirements. Through TTEC and client partnership and strong collaboration will result with eliminating risks and returning to "business as usual" status, and more.

2.6. Privacy by Design

TTEC Digital accommodates applicable data privacy regimes through bespoke data processing agreements (DPA) with its customers that set forth relevant rights and obligations in the context of the data controller-data processor relationship. TTEC Digital also applies appropriate agreed technical and organisational measures and data privacy safeguards (including intercompany standard contractual clauses) to satisfy the legal requirements and the DPA undertakings.



3. Using The Service

3.1. Ordering and Invoicing Process

Buyers wishing to find out more about this service and how to order should contact Wayne Kay, VP EMEA, at gcloud@ttecdigital.com

3.2. Availability of Trial Service

Availability of Trial Service

NiCE IEX Workforce Management (WFM) is available for trial through the SandcastleCX™ programme, designed to provide organisations with a risk-free, hands-on exploration of NiCE's cloud-based solutions.

The trial service offers the following features and conditions:

- No Cost for Standard Use Cases: The SandcastleCX™ trial is provided free of charge for standard use cases, allowing organisations to evaluate the platform without financial commitment or obligation.
- Customised Sandbox Environment: Each trial participant receives a tailored sandbox environment, leveraging NiCE CXone's AI-enhanced capabilities, including intelligent virtual assistants, predictive analytics, and workforce management tools. The environment is configured to reflect the organisation's specific requirements and key use cases.
- Expert Guidance: A dedicated CX architect is assigned to guide users through the setup, configuration, and exploration of the platform, ensuring that the trial aligns with business objectives and technical needs.
- Flexible Trial Period: The trial period is flexible, offering access for several months. This allows organisations ample time to explore core functionality, integrations, and evolving use cases at their own pace.



- Scalable and Evolving Access: The sandbox environment is designed to grow with the user, initially focusing on day-one requirements and extending to day-two and beyond enhancements, including new features, channels, and capabilities.
- Comprehensive Feature Testing: Organisations can use the trial to test a wide range of features, from basic configuration to advanced integrations, and to validate essential use cases before committing to full implementation.

To initiate a trial, interested parties can contact TTEC Digital via the provided channels to discuss requirements and arrange access to the SandcastleCX™ environment.

3.3. On-Boarding

Onboarding Overview

A structured process to implement NiCE IEX WFM for UK Government organisations, ensuring compliance, security, and operational readiness. Activities include planning, configuration, integration, testing, training, and go-live support aligned with G-Cloud and UK Government Cloud Security Principles.

Objectives

- Define scope and deliverables.
- Configure WFM environment for compliance.
- Integrate with ACD and HR systems.
- Train users and drive adoption.
- Provide post-go-live support and transition to steady state.



Roles

- Customer Project Lead: Requirements, approvals, coordination.
- TTEC Digital PM: Governance, timelines, communication.
- NiCE Consultant: Configuration, integrations, security.
- Customer IT: Connectivity, access, compliance checks.
- Workforce Manager: Validate forecasting and scheduling.
- Training Lead: Deliver role-based training and change management.

Phases & Timeline (6–7 Weeks)

1. Scope Definition – Kick-off, requirements, risk assessment. *(1 week)*
2. Design & Build – Configure WFM, ACD integration, security. *(2–3 weeks)*
3. Testing & Validation – ITP, UAT, performance checks. *(1 week)*
4. Deployment & Cutover – Migration, SmartSync, validation. *(1 week)*
5. Training – Concurrent with Phase 4.
6. Hypercare – Post-go-live support for 5 days. *(1 week)*

Deliverables

- Scope document
- Configured WFM environment
- Integration setup
- Test reports (ITP/UAT)
- Training materials
- Hypercare summary

Compliance

- UK GDPR, ISO 27001, SOC2
- UK Government Cloud Security Principles
- UK/EU data residency confirmed



Benefits

- Rapid Deployment – Minimise disruption
- Operational Readiness – Fully tested environment
- User Adoption – Comprehensive training
- Compliance Assurance – Security embedded throughout

3.4. API

NiCE IEX Workforce Management (WFM) provides a robust set of APIs to enable secure, scalable integration with external systems. These APIs support automation, data exchange, and workflow optimisation for UK Government contact centres, ensuring compliance with G-Cloud and UK Government Cloud Security Principles.

API Types and Functions

- SmartSync REST APIs
 - Facilitate real-time data exchange between NiCE IEX WFM and third-party applications.
 - Support JSON, XML, and pipe-delimited formats.
 - Common use cases: schedule exports, adherence data retrieval, and agent performance reporting.
- Export APIs
 - Enable extraction of agent schedules, historical adherence, and payroll data.
 - Configurable for date ranges and cadence (daily or weekly).
- CXone Platform APIs
 - Broader API set for NiCE CXone, including:
 - Authentication APIs for secure login.
 - Admin APIs for managing agents, skills, and address books.
 - Real-Time Data APIs for dashboards and live monitoring.
 - Reporting APIs for historical performance data.



Integration Scenarios

- HR and Payroll Systems: Automate leave and shift data sync with platforms like Oracle HCM or SAP.
- CRM and Case Management: Connect WFM with Salesforce or ServiceNow for unified citizen engagement.
- UCaaS and Telephony: Integrate with ACD systems (e.g., Genesys, Avaya) for real-time adherence and scheduling.

Security and Compliance

- All APIs use HTTPS with TLS 1.2 or higher.
- Authentication via OAuth2/OpenID Connect or secure tokens.
- Data in transit encrypted; fully compliant with UK GDPR and UK Government Cloud Security Principles.

Developer Support

- Comprehensive Documentation: Available in PDF and online formats.
- Sandbox Environment (SandcastleCX™): Provided for testing integrations before production.
- Developer Programme (DEVone): Access to SDKs, tutorials, and community support.

Benefits for UK Government

- Automation: Reduces manual processes and improves accuracy.
- Flexibility: Seamlessly integrates with existing government systems.
- Scalability: Supports future digital transformation initiatives.

Customer Responsibilities

- Ensure API usage aligns with organisational security policies.
- Manage API keys and credentials securely.
- Validate integration through testing before production deployment.



3.5. International SMS

NiCE IEX WFM, as part of the NiCE CXone ecosystem, supports international SMS messaging to enable proactive and responsive communication with agents and stakeholders across global locations. This capability is designed to complement workforce management processes by delivering notifications, alerts, and updates securely and efficiently.

Key Features

- Outbound SMS Notifications
 - Send schedule updates, shift reminders, and adherence alerts to agents internationally.
 - Supports long codes and short codes for global delivery.
- Inbound SMS Responses
 - Agents can confirm or respond to schedule changes via SMS, enabling two-way communication.
- Global Reach
 - Utilises NiCE CXone's SMS aggregation service or integrates with approved third-party SMS providers for international delivery.
 - Configurable for multiple regions to meet local telecom regulations.
- Integration with WFM
 - SMS notifications triggered by WFM events such as schedule changes, overtime requests, or intraday adjustments.
 - API-driven integration for custom workflows.

Compliance and Security

- UK Government Standards
 - Fully compliant with UK GDPR and UK Government Cloud Security Principles.
 - Data encrypted in transit (TLS 1.2+) and at rest.
- International Regulations



- Supports country-specific compliance for SMS delivery, including opt-in/opt-out requirements.
- Authentication
 - Secure API keys and OAuth2 for SMS integration.

Technical Requirements

- Licensing: Requires NiCE IEX WFM with CXone Digital capabilities.
- Rate Limits: Configurable based on provider; typically capped for high-volume international messaging.
- Integration: APIs available for HR, CRM, and case management systems.

Use Cases for UK Government

- Agent Notifications: Shift confirmations, schedule changes, and adherence alerts.
- Emergency Communications: Rapid alerts for service disruptions or critical updates.
- Engagement Campaigns: Surveys and feedback collection for workforce optimisation.

Customer Responsibilities

- Ensure compliance with local telecom regulations for international SMS.
- Manage opt-in/opt-out processes for recipients.
- Validate integration and test workflows before production deployment.

Benefits

- Global Workforce Connectivity: Keep agents informed across borders.
- Secure and Compliant: Meets UK Government and international standards.
- Operational Efficiency: Reduces manual communication and improves responsiveness.



3.6. Off-Boarding

TTEC Digital follows a structured, compliance-driven process to ensure a smooth, secure, and transparent transition when a customer contract ends.

The approach typically includes:

1. Transition and Knowledge Transfer

- TTEC Digital initiates a comprehensive knowledge transfer to the new provider or the client's internal team. This involves meetings with the Client Success Manager, Solutions Architect, and other key resources familiar with the customer's environment.
- All operational and technical documentation, such as call flows, IVR pathing, and integration details, is updated and handed over to ensure continuity.

2. Data and Artifact Transfer

- All customer data, records, and artifacts are securely transferred to the client or their nominated supplier within 30 days of notification, in line with contractual obligations and data retention requirements.
- Strict protocols are applied to maintain data integrity and security during migration, including encryption and controlled access.

3. Access Revocation and Account Closure

- TTEC Digital ensures timely removal of user accounts and system access for its staff from client environments, including CRM, collaboration tools, and cloud platforms.
- Federated identity management (e.g., via Okta and SAML) is used to enforce secure offboarding and prevent residual access risks.

4. Compliance and Data Privacy

- Offboarding aligns with GDPR and contractual data protection clauses, ensuring that personal and sensitive data is either returned or securely deleted after the retention period.
- TTEC Digital provides written confirmation of data deletion or transfer, maintaining audit trails for compliance.



5. Service Continuity and Exit Planning

- A draft exit plan is prepared early, detailing timelines, responsibilities, and any applicable exit costs.
- Optional transitional support projects may be delivered to minimise disruption, such as temporary hosting or migration assistance.

3.7. Training

Training & Enablement Overview

TTEC Digital ensures rapid adoption and operational readiness for NiCE IEX Workforce Management (WFM) through structured, role-based training aligned with UK Government compliance and accessibility standards.

Objectives

- Equip managers, supervisors, and agents with WFM skills.
- Drive adoption via change management and continuous learning.
- Ensure compliance with UK Government security and accessibility requirements.

Roles

- Customer Project Lead: Approves training plan, coordinates resources.
- TTEC Digital Training Lead: Designs curriculum, delivers sessions.
- NiCE Specialist Trainer: Provides product expertise.
- Workforce Manager: Validates outcomes and supports adoption.

Training Components

- Role-Based Training
 - Managers: Forecasting, scheduling, reporting.
 - Supervisors: Intraday management, adherence monitoring.
 - Agents: Self-service portal for schedules and requests.



- Hands-On Enablement: Live environment exercises and real-world simulations.
- Change Management Workshops: Adoption strategies and communication plans.
- Digital Learning Tools: NiCE Learning Portal, Dojo, and TTEC RealPlay™ AI coaching.

Delivery Options

- Instructor-led (onsite or virtual)
- Self-paced online modules
- Blended learning for flexibility

Timeline (3–4 Weeks)

1. Needs Analysis – Assess roles and skill gaps (*3–5 days*)
2. Curriculum Development – Tailored training plan (*1 week*)
3. Training Delivery – Instructor-led sessions and workshops (*1–2 weeks*)
4. Post-Go-Live Support – Hypercare and Q&A (*1 week*)

Deliverables

- Training plan and schedule
- Role-specific materials
- Access to NiCE Learning Portal
- Post-training evaluation report

Compliance

- WCAG accessibility standards
- UK GDPR and UK Government Cloud Security Principles

Benefits

- Rapid Adoption – Faster time to proficiency
- Operational Readiness – Fully trained workforce
- Continuous Learning – Ongoing digital enablement

3.8. Implementation Plan

TTEC Digital delivers NiCE IEX Workforce Management (WFM) implementations using a five-phase methodology designed to ensure clarity, efficiency, and compliance with UK Government standards. Each phase includes defined deliverables, milestones, and project management oversight from initiation to closure.



Implementation Phases

Phase 1: Initiate & Define

- Activities
 - Assign project team and transition from sales to delivery.
 - Issue welcome letter with setup instructions, key links, and contact forms.
 - Conduct Kick-off Meeting with full project team (including sponsors and business users).
 - Provide NiCE Playbook for design documentation.
 - Schedule system review and design workshops.
- Deliverables
 - Project Initiation & Planning Tasks.
 - Kick-off Meeting and Design Workshops.
 - Genesys/NiCE Playbook, Call Flows, Prompt Lists.
 - Preliminary Test and Training Plans.



- Voice Readiness Assessment (if applicable).
- Milestone: Design Approval.

Phase 2: Build

- Activities
 - Configure NiCE IEX WFM environment and integrations.
 - Complete custom development and unit testing.
 - Perform base functionality testing.
- Deliverables
 - Genesys/NiCE Configuration and Base Testing.
 - Custom Solution Development.
 - Final Test and Training Plans.
 - UAT Script Development.
- Milestone: Configuration and Development Completed.

Phase 3: Test & Train

- Activities
 - Execute QA testing and User Acceptance Testing (UAT).
 - Train-the-Trainer sessions for SMEs, supervisors, and administrators.
 - Prepare end-user training plan.
 - Finalise Go-Live Deployment Plan.
- Deliverables
 - QA Testing and UAT Kick-off.
 - Train-the-Trainer Sessions.
 - End-User Training Plan.
 - Production Deployment/Cutover Plan.
- Milestone: UAT Acceptance and Go/No-Go Decision.

Phase 4: Deploy



- Activities
 - Execute Go-Live Deployment Plan.
 - Migrate data/configuration and enable live traffic.
 - Deliver end-user training during Go-Live.
 - Provide hypercare support for first 1–2 days.
- Deliverables
 - End-User Training.
 - Deployment/Cutover Execution.
 - First and Second Day of Service Support.
- Milestone: Production Usage.

Phase 5: Transition & Accept

- Activities
 - Post-implementation support for up to two weeks.
 - Hand-off to TTEC Digital Support team.
 - Project closure and acceptance.
- Deliverables
 - Post-Implementation Support.
 - Support Orientation and Handover.
 - Project Closure Documentation.
- Milestone: Project Acceptance and Closure.

Project Management and Governance

- Continuous oversight from initiation to closure:
 - Status and planning meetings.
 - Risk and issue management.
 - Budget and schedule control.
 - Change management process.
 - Training and test planning management.



Estimated Timelines

Phase	Duration
Initiate & Define	2–3 weeks
Build	2–3 weeks
Test & Train	2 weeks
Deploy	1 week
Transition & Accept	1–2 weeks
Total Duration: ~8–10 weeks (subject to scope and complexity).	

Benefits for UK Government

- Structured Delivery: Clear milestones and governance ensure transparency.
- Operational Readiness: Comprehensive training and testing before go-live.
- Compliance Assurance: Aligns with UK Government Cloud Security Principles and GDPR.

3.9. Service Management

TTEC Digital's Service Management is fully aligned with the specific scope of work agreed upon with the client and delivered upon completion of that scope. This ensures that all service activities directly support the client's operational and strategic objectives.

The Service Management function is led by a Customer Success Manager (CSM), who acts as the single point of contact for the client.

The CSM's responsibilities include:

- Support Oversight: Managing day-to-day support activities and ensuring timely resolution of issues.
- Escalation Management: Serving as the escalation point for critical incidents and coordinating internal resources to resolve them quickly.



- **Commercial Administration:** Handling contractual matters, invoicing, and any financial queries related to the engagement.
- **Reporting and Insights:** Providing regular reports on support activity, performance metrics, and service health to maintain transparency.
- **Client Advocacy:** Acting as the client's representative within TTEC Digital, ensuring their needs and priorities are communicated and addressed across all internal teams.

This structured approach ensures clear accountability, efficient communication, and a proactive partnership model, enabling clients to maximise value from TTEC Digital's services.

3.10. Service Constraints

This section outlines the constraints and dependencies associated with the delivery of NiCE IEX WFM services under the G-Cloud framework. These constraints ensure transparency and help UK Government organisations plan effectively for implementation and ongoing support.

1. Technical Constraints

- **Hosting Environment**
 - NiCE IEX WFM is delivered via NiCE CXone cloud infrastructure; on-premises deployment is not supported.
- **Connectivity Requirements**
 - Reliable internet connectivity is required for all users.
 - Customer must provide secure network access for integrations (e.g., ACD, HR systems).
- **Browser Compatibility**
 - Supported browsers include latest versions of Chrome, Edge, and Firefox.
- **API Usage**
 - Integration via REST APIs requires customer-managed credentials and adherence to NiCE security standards.



2. Implementation Constraints

- Customer Responsibilities
 - Provide accurate and timely information for design workshops and configuration.
 - Ensure readiness of hardware, network, and voice infrastructure prior to build phase.
- Change Management
 - Any scope changes after design approval will require a formal change request and may impact timelines and cost.
- Testing Participation
 - Customer must allocate resources for User Acceptance Testing (UAT) and sign-off before deployment.

3. Training Constraints

- Training Delivery
 - Training is provided in English; translation services are not included.
 - Customer must ensure availability of SMEs and trainers for Train-the-Trainer sessions.
- Accessibility
 - Training materials meet WCAG standards; customer is responsible for any additional accessibility adaptations.

4. Operational Constraints

- Service Hours
 - Standard support hours: Monday–Friday, 09:00–17:30 UK time.
 - Out-of-hours support available at additional cost.
- Maintenance Windows
 - Scheduled maintenance may occur outside business hours; advance notice will be provided.
- Disaster Recovery



- NiCE provides active-active architecture and backup processes; customer must validate DR requirements during onboarding.

5. Compliance Constraints

- Data Residency
 - Primary hosting in UK/EU regions; some support operations may involve offshore access under GDPR-compliant safeguards.
- Security Standards
 - Customer must adhere to NiCE security policies for API keys, user access, and password management.

Benefits of Defining Constraints

- Ensures clear expectations for delivery and compliance.
- Reduces risk of delays and cost overruns.
- Supports alignment with UK Government Cloud Security Principles.

3.11. Service Levels

TTEC Digital provides SLA-backed support and managed services to ensure uptime, compliance, and performance for UK Government organisations.

Availability

- **Platform Uptime:** 99.99% availability via NiCE CXone (excluding scheduled maintenance).
- **Maintenance:** Advance notice; typically outside UK business hours.

Support Hours

- **Standard:** Mon–Fri, 09:00–17:30 UK time.
- **Extended:** Out-of-hours or 24/7 under Managed Services (additional cost).



Incident Response

Severity	Description	Target Response
P1 Critical	Complete outage/severe impact	60 mins
P2 High	Major functionality impaired	2 hrs
P3 Medium	Minor issues	4 hrs
P4 Low	General queries	Next business day

Resolution Targets

- Critical: Fix or workaround within 4 hrs.
- High: 1 business day.
- Medium/Low: 3–5 business days.

Monitoring & Reporting

- Continuous monitoring with automated alerts.
- Monthly SLA reports and root cause analysis for critical issues.

Escalation

Tiered process: Service Desk → Technical Support → NiCE Engineering → TTEC Account Manager.

Financial Recompense

Service credits applied if uptime falls below SLA thresholds.

Customer Responsibilities

Provide accurate contacts and support internal triage/testing.

Benefits

- Predictable Performance: SLA-backed reliability.
- Rapid Response: Defined timelines for critical issues.
- Compliance Assurance: Meets G-Cloud and UK Government standards.



3.12. Outage and Maintenance Management

NiCE IEX WFM is delivered as a cloud-based service under strict Service Level Agreements (SLAs) to ensure high availability and operational continuity for UK Government organisations. Outage and maintenance management processes are designed to minimise disruption, maintain compliance, and provide transparency during scheduled and unscheduled events.

Service Availability

- Standard SLA:
 - 99.9% monthly uptime for NiCE IEX WFM Integrated services.
 - SLA excludes excusable downtime such as scheduled maintenance, emergency maintenance, and outages caused by factors outside NiCE's control (e.g., Force Majeure, internet failures).
- Measurement: Availability is calculated monthly and reported through NiCE's service portal.

Scheduled Maintenance

- Maintenance Windows:
 - Routine maintenance typically occurs:
 - Saturday 10:00 PM to Sunday 6:00 AM EST for NiCE IEX WFM.
 - Additional maintenance for NiCE CXone components may occur Tuesday/Thursday overnight or Friday–Sunday late hours.
- Notification: Customers receive advance notice of scheduled maintenance via email or service portal.



Emergency Maintenance

- **Unscheduled Maintenance:** Performed only when necessary to prevent harm to NiCE systems or customer data.
- **Communication:** Immediate notification provided through standard channels with estimated resolution time.

Incident Handling

- **Monitoring & Detection:** NiCE employs proactive monitoring tools to detect service degradation or outages.
- **Escalation & Communication:**
 - Incident tickets logged in NiCE support systems.
 - Customer notified of status, estimated resolution time, and workaround options.
- **Workarounds:** NiCE may provide temporary solutions if they are more effective than immediate fixes.

Disaster Recovery

- **Architecture:** Active-active network topology ensures resilience and failover capability.
- **Testing:** Quarterly failover drills and annual disaster recovery tests validate readiness.
- **Data Protection:** Backups encrypted (AES-256 at rest, TLS 1.2+ in transit) and stored in geographically redundant locations.

Customer Responsibilities

- Ensure network readiness and compliance with NiCE connectivity requirements.
- Report outages promptly via NiCE support channels.
- Validate configuration changes before production deployment to avoid service disruption.

Compliance & Security

- All outage and maintenance processes align with:
 - UK Government Cloud Security Principles.



- UK GDPR and ISO 27001 standards.
- Data remains encrypted during maintenance activities.

Benefits for UK Government

- High Availability: SLA-backed uptime ensures continuity of citizen services.
- Transparency: Defined maintenance windows and proactive communication.
- Resilience: Disaster recovery and failover processes validated through regular drills.

SLA Summary

Metric	Target
Service Availability	99.9% monthly uptime
Incident Response (Critical)	Within 60 minutes
Scheduled Maintenance Notice	Minimum 5 business days
Post-Incident Report	Within 48 hours of resolution



3.13. Financial Recompense Model for not Meeting Service Levels

- **Service Credits** apply when monthly uptime falls below SLA thresholds:
 - 99.0% – 99.9% uptime: 5% credit.
 - 98.0% – 98.9% uptime: 10% credit.
 - Below 98.0% uptime: 15% credit.
- **Cap:** Credits capped at 15% of monthly subscription fee for the affected service.
- **Conditions:**
 - Credits are not automatic; claims must be submitted within 30 days of outage.
 - SLA exclusions apply for scheduled maintenance, emergency maintenance, and factors outside NiCE's control.
- **Payment Method:** Credits applied to future invoices; no cash refunds.



4. Provision of the Service

4.1. Customer Responsibilities

- Provide accurate requirements and approve scope before implementation.
- Ensure internal resources are available for onboarding, testing, and training.
- Maintain connectivity and access controls for integrations (e.g., ACD, HR systems).
- Validate forecasting, scheduling, and reporting outputs.
- Support change management and user adoption activities.
- Comply with UK Government security and data protection policies.

4.2. Technical Requirements and Client-Side Requirements

- Reliable internet connection with sufficient bandwidth for cloud-based operations.
- Secure network configuration aligned with UK Government Cloud Security Principles.
- Access to supported browsers and devices for WFM portal usage.
- Integration readiness for ACD platforms and HR systems.
- Administrative access for configuration and testing.

4.3. Browsers

NiCE IEX WFM supports modern browsers, including:

- Google Chrome (latest version)
- Microsoft Edge (latest version)
- Mozilla Firefox (latest version)

Note: Internet Explorer is not supported.



4.4. Outcomes/Deliverables

- Configured NiCE IEX WFM environment ready for operational use.
- Validated integrations with ACD and HR systems.
- Role-based training and enablement materials.
- Test reports (Installation Test Plan and UAT sign-off).
- Post-go-live Hypercare support summary.
- Compliance with UK GDPR and UK Government Cloud Security Principles.

4.5. Development Life Cycle of the Solution

- Scope Definition: Requirements gathering and risk assessment.
- Design & Build: Configure WFM instance and apply security controls.
- Testing & Validation: Execute ITP and UAT.
- Deployment & Cutover: Migrate data and validate environment.
- Training & Change Management: Deliver role-based sessions and digital learning.
- Hypercare: Post-go-live support and optimisation. *Total estimated duration: 6–7 weeks (subject to scope).*

4.6. After Sales Account Management

Once you become a TTEC Digital Customer, you will be assigned a Client Success Manager (CSM), who will be responsible for the relationship with your organisation. Your CSM will act as your trusted advisor and will get to know you and your business and help you to identify key strategic objectives to meet your organisational goals. Your CSM will also run regular business/service reviews with you to make sure that we are helping you to deliver effective solutions and will also help you to roadmap your journey to digital transformation. Your CSM is your first point of escalation in times of need. Whilst our teams will align directly with your teams (Project & Programme Management, Service, Support, Procurement, Finance, etc), your CSM will take



overall responsibility for the relationship and communication with your organisation. TTEC Digital's Account Strategy is to make sure that we meet and exceed your expectations. We see the role as a key function to ensure smooth service delivery and to educate, benchmark and challenge the status quo, helping you to drive efficiencies and outstanding Customer Experience wherever possible.

We see effective Account Management as a way to build a long term and valuable partnership with your organisation.

4.7. Termination Process

TTEC Digital is open to entertaining reasonable termination mechanisms as part of the contract negotiation that will account for the specificities of the individual business opportunity and the associated commercial terms.



5. Other Messaging Services

- SMS and messaging capabilities available on a pay-as-you-go basis.
- Integration with third-party messaging platforms via NiCE SmartSync.
- Support for agentless SMS, one-to-one messaging, and inbound queuing.
- Optional BYOT (Bring Your Own Technology) for advanced messaging and bot integrations.



6. Environmental Action and Social Value

6.1. Environmental Action

Global Environmental Governance and Strategy

TTEC manages its environmental impact through a structured governance and operational framework. Oversight is provided by a dedicated Board committee and an Environmental, Social, Governance (ESG) Executive Council. We operate under a formal [Climate Change and Environmental Responsibility Policy](#) and align our disclosures with recognised frameworks, including SASB and TCFD. Our environmental strategy includes initiatives focused on energy efficiency, waste reduction, and emissions tracking, with progress informed by regular materiality assessments.

UK-Specific Environmental Action and Net Zero Commitment

TTEC Consulting (UK) Limited is committed to environmental sustainability and achieving net zero emissions by 2045, ahead of the UK Government's 2050 target. Our UK Executive Team has formally endorsed and published a comprehensive [Carbon Reduction Plan](#) that fully complies with PPN 06/21 and its associated guidance. The plan includes transparent disclosures of Scope 1 and Scope 2 emissions, as well as relevant Scope 3 categories, and is reviewed annually to ensure continued alignment with evolving regulatory standards and net zero objectives. This proactive approach reflects our leadership in climate responsibility and our dedication to supporting public sector clients in meeting their sustainability goals.



6.2. Social Value

Creating Positive Impact for Customers and Communities

At TTEC Digital, we are committed to creating lasting social value that benefits both our clients and the communities they serve. Our efforts focus on tackling economic inequality, advancing equal opportunities, and expanding digital inclusion throughout the UK.

To support this mission, every UK-based TTEC Digital employee is encouraged to participate in corporate social responsibility (CSR) initiatives, with one paid day annually reserved for volunteering and community engagement.

Empowering Youth Through Digital Skills

At TTEC Digital, we believe in leveraging our expertise and partnerships to create opportunities for the next generation. One example is the Digital Dev Academy, a collaborative programme that equips students from underserved communities with essential digital and technology skills. The programme is delivered in partnership with TTEC Digital and its network of clients, with support from local authorities and education stakeholders. Its goal is to create inclusive pathways into technology careers by providing hands-on learning experiences and exposure to real-world digital environments.

We work closely with clients to co-design the curriculum, ensuring it reflects current industry needs and emerging technologies. These partners also contribute mentorship, resources, and opportunities for students to engage with professionals across sectors. Their involvement helps bridge the gap between education and employment, making the learning experience both practical and aspirational.

In parallel, we collaborate with county councils to identify eligible schools and students, coordinate logistics, and ensure the program is accessible to those who need it most. This partnership is vital for community engagement and helps embed the academy within local



development strategies. It culminates in a showcase event where students present their work and explore career opportunities with participating partners. The Digital Dev Academy is a powerful example of how cross-sector collaboration can drive social impact and digital inclusion.

Promoting Fair Employment and Economic Resilience

TTEC Digital is a Living Wage accredited employer in the UK, reinforcing our commitment to fair pay, community resilience, and inclusive growth. This milestone reflects our broader mission to empower future talent, support public sector innovation, and create lasting social impact.

At TTEC Digital, we believe that fair pay fosters a positive and collaborative work environment. By ensuring our employees feel genuinely valued, we strengthen relationships across teams and empower individuals to thrive. This leads to better outcomes for our clients, including:

- More engaged teams focused on solving customer challenges.
- Technical experts who go the extra mile to deliver innovative solutions.
- Project managers who build stronger, more trusting relationships.
- Consultants who invest their full expertise in transforming businesses.



7. Our Experience

7.1. Case Study

The challenge

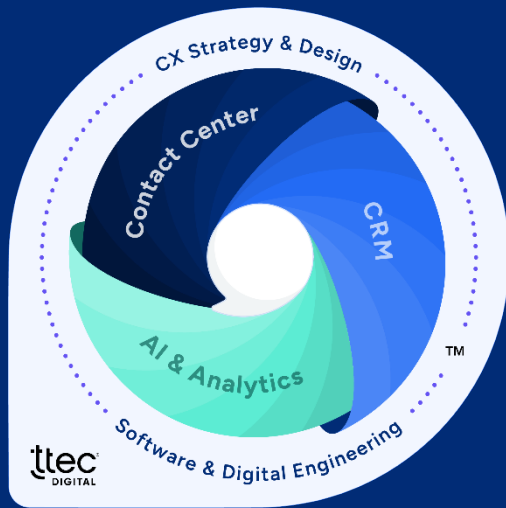
Founded in 2004, a leading provider of administrative healthcare services for federal and commercial clients faced a significant operational hurdle. With administrative costs accounting for up to 40% of total healthcare expenses, their mission is to reduce this burden so clients can focus on care delivery. However, their contact centre faced a major challenge: their legacy telephony system lacked the FedRAMP certification required for federal contracts.

The solution

To meet urgent compliance and performance needs, the organisation selected NiCE as their new telephony platform. When the standard implementation timeline did not align with client demands, NiCE recommended TTEC Digital. Leveraging deep contact centre and FedRAMP expertise, TTEC Digital accelerated deployment and introduced key enhancements, including a self-service IVR, a customised crisis line escalation solution, and quality management tools.

The result

Thanks to TTEC Digital's hands-on project management, technical expertise, and training support, the aggressive implementation timeline was met without compromising quality. The introduction of a self-service IVR and a customised crisis line solution significantly improved call routing and responsiveness, especially for callers in distress. Quality management tools enabled better oversight and performance tracking. Most notably, the transition was so smooth that feedback from the 1,000+ call centre staff was minimal, an indicator of successful change management.



About TTEC Digital

TTEC Digital is a global leader in customer experience orchestration, combining technology and empathy at the point of conversation. Today customer conversations, and the contact centre technologies that support them, are inseparable. We bring decades of innovation experience across the world's leading contact centre technology platforms – and blend it with in-house expertise in CX strategy, data and analytics, AI and more – to help organisations maximise their technology investments and create truly exceptional customer experiences.

Contact Us

Wayne Kay

Vice President, EMEA

Email: gcloud@ttecdigital.com

Website: www.ttecdigital.com