Service Description

Workforce and Duty Management Solutions for G-Cloud 13

Crown Computing Limited

Document Reference:	D991-001-GC13
Date of Issue:	25th April 2022

Introduction

The Crown Workforce and Duty Management (WFM-DMS) solution as a Managed Cloud Service ("the Service") provides a cloud-hosted environment containing all the necessary cloud resources, capacity, and component services to deliver the WFM-DMS application functionality.

This document provides a profile of the overall service and high-level descriptions of component services that lie within the scope of the Managed Cloud Service.

Service Model Overview

Integrated Application and Infrastructure

As a managed cloud service, the Service is designed to provide a comprehensive workforce and duty management solution. The Service provides a self-contained configuration that delivers the WFM-DMS application integrated with the necessary infrastructure capacity, operations, monitoring, and management services.

The Service does not require the customers to provide data centre or data room type of infrastructure to host the WFM-DMS application.

However, the Service provides secure features to support integration with customers' on-premise environments, including:

- File interchange facilities for secure import and export of data for system interfaces
- Web Service APIs for standards-based transaction interfaces
- Secure site-to-site connectivity using encrypted Virtual Private Network (VPN) gateways to support specific requirements such as on-premise user authentication systems, secure connectivity of on-site devices without encryption capability, or other agreed requirements
- Read-only data access for self-service reporting requirements.

Installed functionality and features are subject to the scope of respective service offerings licenced by each customer.

Security and Compliance

The internal systems and processes comprising the Service will be implemented to provide assured security and compliance in accordance with established good practice, standards, and in accordance with Data Protection Legislation. In particular, the key pillars of security and compliance underpinning the Service include the following:

Microsoft Azure Platform	The Service is implemented on the Microsoft Azure cloud platform. Detailed information about Azure compliance offerings are publicly and independently available from the Microsoft Trust Center. Customers can satisfy themselves that the Microsoft Azure platform meets their compliance requirements.
Security Principles	In implementing the Service for customers, Crown has chosen to align its data security principles and policies with the guidance published by the

	UK Government agency, the National Cyber Security Centre (NCSC). This guidance has gained wide recognition and acceptance both within the public and private sectors. In addition to being good practice, it also provides a structured scope of security concerns and a common terminology for communication. The NCSC principles are aligned with ISO 27001 to which Crown is accredited.
UK GDPR	The Service provides a UK GDPR compliant capability and system, exploiting the security measures and privacy policies to safeguard its data, including the categories of personal data identified by the GDPR. Identifying personally sensitive data within the Service and controlling who has access to it is a critical feature of the Service. The Service has the capacity to interface with Customer policies and procedures to manage user identities and credentials and control access to the data. The Customer will be required to enter into a Data Processing Authorisation Agreement in the form scheduled to the Managed Cloud Services Agreement.
Customer Required Compliance	The Service can be installed so that Customer data can be held and processed within specific geographic locations. For UK public sector customers, the UK Crown Commercial Service accepted the Microsoft Azure cloud services classification at Government Cloud (G-Cloud) v6. UK government agencies and partners can use in-scope services to store and process UK government data classified as OFFICIAL, which includes the vast majority of government data.

Transparent Operations and Service Management

When WFM-DMS is installed and configured so that customers can access the application functionality through secure interfaces. The Service infrastructure will be operated, monitored, and managed by Crown.

The internal management of the Service configuration and operations makes use of automation and automated processes to maintain system performance, security, and resilience.

The visibility of internal technical configuration and operation of the service will be restricted to authorised access for audit purposes. Selected elements of configuration and operations will be made available to customers' service representatives through agreed service reporting packs.

Service Delivery

Crown will appoint a named Service Delivery Manager (SDM) with the responsibility for the successful configuration, operation, and delivery of the Services to the Customer business and user community.

The Customer will be expected to provide corresponding Service Representatives for the business and users.

The SDM will engage with the customers' Service Representatives for assuring the successful delivery of Services on an ongoing basis, periodical service reviews, and providing service reports as agreed.

Service Levels and Reporting

The Service can be installed, configured, operated, and managed to meet the requirements of the Customer's business.

A number of specific key metrics that are appropriate will be formally agreed, covering:

- Service Availability – reflecting the functional availability of the overall WFM-DMS service to the users
- System Performance – reflecting the performance of the overall system configuration to deliver responsive interactive transactions and timely background processing
- Service Restoration – covering the management of service continuity through periods of potential disruption due to infrastructure problems and failures
- Support Performance – reflecting the performance of the Crown Customer Support services in addressing incidents and service requests

System Metrics

It is important to understand the scope and applicability of these metrics:

- Availability and performance metrics relate to the overall configured service, and not to those of component systems and services. The Service is designed to maximise availability and performance irrespective of individual components.
- Availability, performance, and restoration metrics will be applicable to the cloud-based installation of the service. Corresponding performance of Customer's own infrastructure, systems, and processes that are involved in the delivery of functionality to the Customer business and users will be out of scope for these service metrics. The design of the system within the Service includes facilities and provisions in the cloud environment for monitoring and measuring these metrics.

Component Cloud Services

The Service includes a number of component cloud services that are used to host the WFM-DMS application and deliver its functionality to the Customer. The key cloud components are described in this section.

Cloud Platform

Customer Environment

The Service will be implemented on the Microsoft Azure cloud platform (Cloud Platform), with the WFM-DMS application being hosted within a dedicated compartment for each customer, isolated from other customers as a virtual private Cloud.

Each customer gets a distinct and separate tenancy in the cloud, with customer-specific application, database, and configurations. Customers are isolated from other cloud tenants at network level, and operationally independent from other customers. This environment will be accessible by authorised users in the Customer's organisation. It can also be connected to the customer's on-premise environment through mutually agreed secure and encrypted links.

The Service will include the provisioning, operation, and management of the technology components required for hosting the WFM-DMS application. These components will be deployed and delivered as an integrated Service.

Cloud Subscription

Crown will procure and operate the necessary Azure account and subscription from Microsoft on behalf of the Customer to specifically host the WFM-DMS application. This Azure subscription will be distinct and separate from any other Azure or other cloud account or subscription that the Customer might have implemented.

Compute Infrastructure

The Service will provision, operate, and manage the required number and sizes of virtual server machines (VMs) for the following purposes:

- Web Servers, to provide the primary user access functionality of WFM-DMS web applications
- Terminal Servers, to provide remote desktop and applications
- Device Control Servers, for interfacing on-premise clocking terminals
- File Transfer Servers, to provide access to files for interfaces to external systems, and reports
- Application Servers, to provide background functional processing of WFM-DMS functions
- Domain Controllers, to provide local directory services for the Customer environment; and
- Database Servers

Internal Service Management

The Service will include the following service management processes:

Update	The most recent supported version of Microsoft Windows Server and Microsoft SQL Server, tested and validated by Crown, will be initially installed and configured. Thereafter, the environment will be maintained and updated to subsequent versions under internal change control procedures.
Capacity	The number and/or size of VMs will be dynamically managed to support performance objectives.
Availability	The VMs will be capable of service healing. In case of any failures in the underlying hardware, the VMs will be automatically re-provisioned. In higher availability configurations, workloads will be automatically redistributed to additional VMs configured on separate underlying infrastructure.
Identity and Access Control	VMs will be located and secured within the local Active Directory and user authentication services.
Security	Antimalware will be installed and operated on all VMs Virus signatures will be continuously updated Antimalware engine will be updated periodically

The availability of the overall Service will be managed using redundant infrastructure to protect against outages of component services.

Storage Infrastructure

Within the Service, all the VMs will be automatically provisioned with the necessary storage using virtual hard disk technologies on the Cloud Platform. Additional storage will also be provisioned for storage of WFM-DMS data as required for databases and file storage.

Internal Service Management

The Service will include the following service management processes:

Backup	• All data in the Service will be backed up regularly to Azure Recovery Services Vaults using the Azure Backup Service • Recovery Services Vaults will be created within the Customer environment • The backed-up data will include VM images, file data, and databases

Capacity	All the disk capacity required for the Service will be provisioned on solid-state VHDs within the required geographic location
Availability	The VHDs will be capable of service healing. Disk data will be held in multiple replicas. In case of any failures in the underlying hardware, the VHD replicas will be automatically re-provisioned and availability maintained. In DR configurations, data will be automatically replicated to the secondary data center.
Security	• All disks will be mandatorily encrypted to protect data-at-rest • The WFM-DMS database will be additionally encrypted using Transparent Data Encryption (TDE) feature of SQL Server

Network Services

Virtual Networks

The Customer's infrastructure resources will be defined within dedicated Virtual Networks (VNets) with private IP address spaces. All resources of the Customer environment will be located within those VNets, segmented into subnets.

Subnets

The Crown WFM-DMS application implements a multi-tier architecture consisting of:

- **Access/Application Layers**, providing a secure doorway to the application and housing the core functionality of the application; and
- **Database Layer,** containing the core operational databases of the application.

Each layer of the architecture is implemented in its own subnet, and each subnet is protected by firewalls.

VPN Gateway

The Service design includes the capability for secure and encrypted connectivity between the customers' own on-premise networks and the cloud through VPN Gateways.

This allows site-to-site connections from customer locations and the cloud environment on Azure over the internet or direct connection using Virtual Private Network connectivity, extending the customer networks into the Cloud Platform.

Access Control Lists (ACLs) and Firewalls

The Service uses a complex of multiple Access Control Lists (ACLs) and Firewalls to protect the Customer's environment in the cloud to restrict access to resources. Where there are multiple production environments, these Access Control Lists (ACLs) and Firewalls will also be integrated with load-balancing functionality to provide relocation of workloads away from any failing servers to maintain higher availability.

Internal Service Management

The Service will include the following service management processes:

Capacity The overall network configuration will be sized and dynamically adjusted to support the evolving network flows.

Security The network will be protected by a sequence of firewalls in tandem, with the application data protected against access from the internet.

Operating Environments

Production Environments

The Service can include a set of agreed production environments, sized and configured as agreed.

At least one production environment must be specified for a customer environment in the cloud, as it will contain some common services that could be used by other non-production environments.

Non-Production Environments

In addition to the production environments, the Service can optionally include non-production environments with application images for testing and training purposes.

Non-production environments will only be covered by service level commitments relating to provisioning lead times.

Subject to agreed service charges, non-production environments will be billed by operational periods that they are made available for.

Test and training environments are usually functional representations of production environments on reduced-scale and simplified configurations to keep the costs to a minimum. In some cases, full-scale, full-configuration images might be required for pre-production or non-production purposes.

Customer Support Services

Customer Support

Key Roles

There are 6 key roles in Crown that facilitate the assured delivery of services and support to customers:

Service Delivery Manager	The Service Delivery Manager (SDM) will be responsible for the operational delivery of Crown solutions and services to the Customer. The SDM will also be the responsible contact for major incident management. The SDM reports to the Head of Customer Support.
Project Manager	The Project Manager is responsible for the management of implementation and change projects for the Crown services. Following the completion and closure of the project, operational delivery responsibility is handed over to the SDM. The Project Manager reports to the Head of Projects and Professional Services.
Support Manager	The Support Manager is responsible for the delivery of all support services including the Crown Service Desk. The Support Manager reports to the Head of Customer Support.
Head of Customer Support	The Head of Customer Support has the overall responsibility for the service management and customer support organisation within Crown, and as such is the point of escalation for the Customer.
Head of Projects and Professional Services	The Head of Projects and Professional Services has the overall responsibility for the management and delivery of projects to Crown customers, and consulting services relating to the Service.
Client Account Executive	The Client Account Executive has the responsibility for maintaining the business relationship between the Customer and Crown.

Service Desk

The Service Desk is the first line of contact for users to request problem support, service support, advice, and guidance on the use of the Service.

Ticket Management

The Ticket Management process facilitates the management of the registration, categorisation, and resolution of open tickets reported by customers relating to Crown's products and services.

User requests for service assistance can be registered with the Support Desk by telephone, email, or through the Customer Services website. All requests will be assigned a unique ticket number for categorisation and tracking of requests through resolution.

Following initial investigation, Crown will categorise open tickets to one of the following categories:

- Pending, subcategorised by required resolution step
- Request for Change (RFC), subcategorised by status
- Service Defect, subcategorised by resolution status
- Hardware Faults, for Clocking and Access Control devices under Crown support
- Advice on service implementation, usage, and configuration

The users may view their open tickets via the Customer Services Website.

Tickets will remain open for up to three months of resolution, unless otherwise agreed with the Customer. If the resolution requires Crown to issue a software correction, the ticket will stay open until the software correction has been applied to the Service.

Remote Support

Crown support staff might need to use Remote Support technologies to work with the users in investigation and resolution of problems. The choice, use, and security of remote support technologies will be agreed with the Customer during initial implementation.

Out-of-Hours Support

Support and service requests outside of standard hours may only be provided by prior arrangement. Such arrangements usually consist of a Standby fee for arrangement, and charges as incurred out-of-hours.