REDCENTRIC

HOSTED DESKTOP SERVICE SERVICE DEFINITION

SD063 / V2.0
Issue Date: 06 July 2018

redcentric
business technology. managed.

1) OVERVIEW

Redcentric's Hosted Desktop Service (HDS), often referred to as VDI or desktop as a service, provides Customers with Microsoft Windows desktops hosted on a Redcentric managed VMware Horizon View infrastructure, within Redcentric's data centres. These desktops can be accessed remotely by the Customer from a mixture of client devices and locations.

HDS is delivered in Customer dedicated instances and can operate as a single or dual site solution.

HDS support scaling the number of defined and concurrent users throughout the life of the service.

2) SERVICE DESCRIPTION

HDS provides desktop services for Customers, hosted within Redcentric's data centres, with the option for single or dual site deployments.

2.1) ASSOCIATED SERVICES

HDS is complementary to Redcentric's Infrastructure as a Service (IaaS) providing a desktop environment to access hosted server environments.

HDS focuses on the delivery of desktops and will be consumed with other Redcentric services to enable access to the desktops, such as:

- Internet & WAN layered bandwidth
- N3 and secure remote access services

2.2) FUNCTIONALITY

2.2.1) PARAMETERS

HDS is delivered within the parameters defined in this service definition.

2.2.2) DESKTOP ENVIRONMENT

HDS provides a virtual desktop environment that hosts the Customer's desktops within Redcentric's data centres. Each desktop utilises Microsoft Windows Desktop operating system and is accessible remotely, via a network connection, from the user's computer. The connection between the user and desktop is encrypted and 2-factor authentication can additionally be utilised to provide further logon security into the HDS environment.

The desktop provides an environment to run the Customer's applications.

HDS will be delivered to meet Customer specific requirements for the:

- Microsoft Windows Desktop operating system version (Windows 7 onwards)
- Number of defined users authorised to access HDS
- Concurrent number of users, including disconnected sessions, accessing HDS
- Number of desktops pools required within HDS to meet the needs of different user work profiles, such as:
    - permanent or floating desktop types, or
    - desktop specifications (CPU, RAM), or
    - different applications installed in to the desktop build
- Number of persistent (permanent) and non-persistent (floating) desktops required within HDS

This is explained in the following hypothetical example:

Customer	Customer X
Scenario	Customer X has 4,500 employees that require access to the corporate desktop. The Customer is an organisation with the following worker profile: • 1,000 users are office based, working Monday to Friday between 9am and 5pm. They require access to Microsoft Office Standard edition and typically have between 1 and 5 applications open, with regular use. The group consists of many part time workers, leading to at most 600 users concurrently accessing their desktop. • 3,000 users are office based, working 24x7 in a five team shift pattern. They require access to Microsoft Office Professional edition and typically have 5+ applications open with regular use. Due to the shift pattern with some overlap, at most 800 users concurrently accessing their desktop. • 500 users are a mix of office and home based, working Monday to Friday between 8am and 6pm. They require access to Microsoft Office Professional edition and bespoke software with 5+ applications open with intensive use. The users will regularly leave their desktop running overnight to complete batch work activities. The mix of home working and disconnected sessions leads to at most 400 users concurrently accessing their desktop.
Redcentric HDS solution	HDS service designed to support 4,500 defined users, split into three desktop pools, with the following parameters: • **Pool 1** – Support 600 concurrent desktops and 1,000 defined users. The users will be assigned a desktop on logon from a floating pool, which will be returned to the pool on logoff. The desktop will be assigned 2 CPU cores and 2GB RAM to support the user profile. • **Pool 2** – Support 800 concurrent desktops and 3,000 defined users. The users will be assigned a desktop on logon from a floating pool, whilst will be returned to the pool on logoff. The desktop will be assigned 2 CPU cores and 4GB RAM to support the user profile. • **Pool 3** – Support 400 concurrent desktops and 500 defined users. The users will be assigned a desktop permanently on logon. The desktop will be assigned 2 CPU cores and 8GB RAM to support the user profile.

2.2.2.1) Desktop Specification

The desktop specification can be varied per desktop pool with the following options commonly used:

User description	Use	CPU cores	GB RAM	Steady State Disk IOPS	Kbps Network Bandwidth (Optimised)
Task-based	1-5 applications / light	1	1	7	50
Knowledge	1-5 applications / regular	2	2	16	100
Power	5+ applications / regular	2	4	25	400
Power+	5+ applications / intense	2	8	40	600

The desktop operating system utilised additionally affects the desktop specification with the following:

Desktop operating system	CPU cores	GB RAM	GB system disk
Windows 7 Enterprise / 32 bit	1 min	1 min	24 min
Windows 7 Enterprise / 64 bit	2 min	4 min	32 min

2.2.2.2) Desktop Persistency

HDS supports persistent and non-persistent desktops, with the functional differences listed in table below. Non-persistent desktops, also referred to as floating, is assigned to the user for the period of logon and then returned to the desktop pool. A persistent desktop, also referred to as permanent, is assigned to the user permanently on first logon from a pool of available desktops. Floating desktops are utilised as the default for HDS.

	Persistent	Non-persistent
Applications deployed as part of base (Gold) image	First logon, or via forced desktop recompose at logon	Yes, via desktop recompose at logon
Applications deployed as part of VMware ThinApp	Yes	Yes
Mapped network drive for user file storage	Yes	Yes
Windows profiles and persona management used	Yes	Yes
Can user install their own applications, if policy allows	Yes	Yes
Are user installed applications maintained between logons	Yes	No
Desktop deployed from Gold image on user logon	First logon only	Yes

A floating desktop has the benefit of reducing the desktop management overhead compared to permanent desktops. Permanent desktops are beneficial where the use requires specific features, such as the ability to self-install software onto the desktop OS drive and not lose this after logoff. Any customisations made to a floating desktop will be lost on logoff, such as application installation.

2.2.2.3) Desktop Pools, Defined Users and Desktop Concurrency

HDS allows creation of separate desktop pools to support delivery of different desktops to different groups of users. The reasons to create separate desktops pools includes:

- Different applications installed into the base (Gold) image
- Different desktop specification (CPU cores, RAM, etc.)
- Floating or permanent desktop assignment
- Security boundary for desktop and onward environment

When a user connects into the HDS environment, they will be able to select desktop connections from desktop pools to which they have been authorised.

Each pool is created with a finite number of deployed desktops. For floating desktop pools, desktops are assigned to users on logon and then return to the pool on logoff, consequently the pool will have sufficient deployed desktops to meet the concurrent access levels. For permanent desktops pools, desktops are assigned on first logon and therefore removed from the pool capacity for the lifespan of the user on HDS, consequently the pool will have sufficient deployed desktops to meet the number of defined users.

Powered on desktops will consume HDS host CPU and memory resources, whether logged on or not, therefore affecting the desktop concurrency within HDS. To manage the number of powered on desktops, Redcentric will:

- Suspend desktops on user logoff
- Force disconnected desktops to logoff and suspend after 5 days

HDS does not limit the number of concurrent access, other than to the number of deployed desktops within a desktop pool.

2.2.3) Customer Applications

Customer desktops within HDS are deployed from a master desktop build, referred to as a Gold image. The Gold image is a template used by HDS to deploy a new desktop into the desktop pool, prior to the user's first logon. The Gold image contains the desktop operating system and Customer applications.

Additional applications can be streamed into the desktop via VMware ThinApp from a local file store within HDS. The applications are not installed local to the desktop but run within the desktop operating system.

Upon logon to the desktop the user will be presented with a desktop environment that contains Customer applications installed as part of the Gold image and Customer applications streamed via VMware ThinApp.

Multiple Gold images may be required to support the Customer's user case requirements.

Management of licences for Customer applications will be the responsibility of the Customer.

2.2.3.1) Customer Application Deployment

Customer applications can either be installed as part of the Gold image or packaged for delivery via VMware ThinApp. The Customer will specify which deployment method is required for each new application deployment.

Customer application deployment requests will be submitted to Redcentric who will raise a change within its service management system. Change approval will be required in the following scenarios:

- Pilot an application deployment within a Gold Build
- Production rollout of a new Gold Build
- Pilot and production rollout of a Thin App Customer application deployment

Applications contained within the Gold image will be available to all desktops that are deployed from that Gold image. Persistent desktops will pick up Gold image contained applications on first logon/deployment, or via a desktop recompose as part of a logoff/logon for Gold image updates. Non-persistent desktops will pick-up Gold image contained applications on each logon.

Applications packaged up for delivery via VMware ThinApp are deployed on logon for both persistent and non-persistent desktops. Access to the application is controlled via membership of Microsoft Active Directory Security Groups and can be deployed on an as-needed / authorised basis.

Beyond the service activation, Redcentric can package up applications into the Gold image or as VMware ThinApps as a chargeable service. This will be logged via Redcentric's support desk as a service change and will be assigned a priority that affects the lead-time to work on the request. Target lead-times for the delivery of change are as follows:-

- New Gold Build (from receipt of formal request) = 15 working days.
- New Thin App or update to existing Gold Build (from receipt of formal request) = 5 working days.
- Lead-time required to commence roll-out of Gold Build = 2 Working Days

Redcentric's service level for service requests are based on Severity 5 incidents (7 calendar days) and will be used to manage build changes.

2.2.4) Client Software

HDS can be accessed from the users' computer utilising either a software client installed locally. The software client provides a rich user experience and is the preferred access method.

The software client utilises VMware's View client that can be downloaded from https://www.vmware.com/go/viewclients.

2.2.5) User Authentication and Connection Security

User access to HDS utilises Microsoft Windows Active Directory (AD) authentication.

2-factor authentication (2FA) can be added to HDS, as a chargeable option, to improve the logon security and is used wherever access to secure environments, such as N3, is required.

Redcentric will provide a Customer dedicated AD domain as part of the HDS service activation. The AD domain will be used for the purposes of controlling access to:

- All HDS desktop pools
- User and shared file stores
- VMware ThinApp delivery to the desktop at user logon

Initial connection to the desktop from the client will utilise HTTPS over TCP/IP to establish and authenticate the user. The subsequent communication between the client and the desktop session will utilise VMware PC over IP (PCoIP) which communicates over UDP, with AES 256 bit encryption.

2.2.6) Desktop Security Policies

Redcentric will apply a base desktop security policy on HDS of:

- Users will not be placed in the local administrators group
- Not allow users to install their own software
- Set minimum password length, complexity, and screen lock-out time of 15 minutes.

Additional security policies can be applied as part of HDS service activation and could include:

- Block paste into the HDS desktop from the client computer
- Block copy from the HDS desktop to the client computer
- Block USB pass-through into the HDS desktop for client computer connected devices
- Block internet access.
- Apply other security in accordance with the Customer's Audit Policy.

2.2.7) Anti-Virus

Redcentric can provide Sophos anti-virus software within each HDS desktop, as a chargeable option. The anti-virus software would be configured with the following policies:

- On access scanner: Scan executable, known vulnerable and also files with no extensions on all drives
- Device control: Block access to all removable drives (by default)
- Check for updates every 15 minutes

2.2.8) User and Shared File Stores

Redcentric will provide user file store for each desktop within HDS of an agreed per user capacity, i.e. 10GB. The user file store will operate as a mapped network drive and will be private to each user.

2.2.9) Desktop Operating System Patching

Redcentric will patch the Gold image, such that new or deployed desktops will receive updates. Redcentric will use the desktop recompose feature for deployed desktops and will require the user to logoff and logon to pick up the update.

Redcentric will not apply patches to Customer applications deployed within the Gold image or ThinApp unless specifically requested by the Customer.

The patching process followed will be:

- The Customer nominates a number of users for patch testing
- Redcentric identifies patches to apply and passes to the Customer for approval
- The Customer reviews and authorises patches to be applied
- Redcentric raises a change to approve the pilot of an updated Gold Build
- Redcentric clones the Gold images within HDS and applies patches via a local Microsoft Windows update service
- Redcentric applies the patches to the Customer nominated users for patch testing
- The user users logoff and logon to pick up the patches and work with patched desktops for 1 week
- Redcentric raises a change to approve the rollout to production of the updated Gold Build
- Redcentric applies the patches to remaining users' desktops via a desktop recompose feature
- All users logoff and logon to pick up the patches applied to the Gold image

If HDS is affected due to the Customer's non authorisation of a Redcentric recommended patch, then the service level and consequent service credits due may be reduced.

2.2.10) HDS Platform Patching

Redcentric will patch the HDS platform quarterly, except where critical patches are released from the vendors and are assessed and approved as critical.

Patches will be applied to primary HDS platform first and then the secondary HDS platform one week later, for dual site HDS deployments. If a fault is recognised as part of the primary HDS platform update, the Customer will failover to the secondary HDS platform, whilst Redcentric investigate and resolve the fault.

Patches will be applied during working hours, i.e. Monday to Friday 8:30am to 5:30pm when full support is available from Redcentric.

2.2.11) Printing

Redcentric can allow or block pass-through of client connected printers, both local and network mapped, into the desktop by policy.

2.2.12) Software Licences

Redcentric will provide licences with HDS for each desktop to cover:

- VMware View

Redcentric will provide licences to support delivery of the HDS platform covering:

- Microsoft Windows Server
- Microsoft SQL Servers
- VMware vSphere

Redcentric may at its discretion update the software versions in use during the contract term.

The Customer will be responsible for ensuring that it has valid Microsoft Windows Virtual Desktop Access (VDA) rights as part of its end user licence agreement with Microsoft for all defined users within HDS.

2.2.13) Reporting

Redcentric does not provide automated reporting as part of HDS, such as current desktop connections, number of desktops, file storage consumed. This information can be provided at the request of the Customer ad-hoc, and will be presented on a monthly service report.

2.2.14) Network Access

HDS can be made accessible to Customer over various network, such as Internet, MPLS WAN or N3 as part of a complementary service provided by Redcentric. The network access requirements and methods will be defined as part of the HDS presales activities.

HDS network bandwidth ranges from 50Kbps to 2Mbps per desktop depending upon the use case. For an optimised office productivity desktop, with no video or 3D graphics, the range is 50-100Kbps per desktop.

2.2.15) Single or DUAL Site HDS

HDS can be delivered as a single or dual site service, both to a defined SLA and SC regime.

A dual site deployment offers a higher level of service availability and operates as an active / passive service over two sites. The dual site HDS service provides the following features:

- Active / passive HDS platform at two Redcentric data centres
- Two uniform resource locator (URL) addresses covering primary and secondary data centres
- In the event of either primary or secondary HDS platform unavailability the user can specify the appropriate URL
- Persistent desktops are not replicated between data centres. Any local configuration changes made to a user's desktop (installing local applications) will not be transferred between live and recovery
- User file stores, shared file stores and desktop profiles will be replicated between data centres
- Users will connect and authenticate into HDS and then be presented with desktops they are authorised to access, i.e. primary or secondary desktops
- Users will connect into either primary or secondary URL to get access to desktops
- Disaster recovery tests can be performed at any point in time by connecting to either primary or secondary HDS platforms

2.3) CUSTOMER DEPDENCIES

The following Customer dependencies apply to HDS:

- The Customer will provide licences, installation media and installation guidance, for applications running within the desktops hosted on HDS
- The Customer will provide the client device, whether computer or smart-device, to initiate the desktop connection from
- The Customer will obtain Microsoft Windows Virtual Desktop Authorisation (VDA) right, or equivalent licence to cover all defined users within HDS
- The Customer will authorise defined user requests on HDS
- The Customer will approve desktop patches, nominate users for patch testing and provide feedback on any adverse metrics
- The Customer will provide desktop support of users within HDS

2.4) EXCLUSIONS

The following exclusions apply to HDS:

- HDS does not allow users to install their own applications into the desktop environment
- Users will not be able to create new users or desktops
- Users will not have local administrator access to the desktop operating system

2.5) ROLES AND RESPONSIBILITIES

The following table details roles and responsibilities that apply to HDS.

Service	Task	Who
User Management		
HDS	Log HDS support calls from users	Customer
HDS	Provide help & advice to users	Customer
HDS	Escalate issues to Redcentric	Customer
HDS	Update / delete / suspend HDS users (Service Request)	Customer
HDS	Unlock Windows user accounts	Supplier
HDS	Create new HDS users	Supplier
HDS	Update / delete / suspend HDS users	Supplier
HDS	Reset windows user password	Supplier
HDS	Own & maintain the user creation process	Supplier
HDS	Approve new HDS users / changes	Customer
Service Management		
HDS	Order additional HDS capacity (to meet new requirements)	Customer
HDS	Monitor the service	Supplier
HDS	Fix service issues	Supplier

Service	Task	Who
HDS	Implement change requests	Supplier
HDS	Undertake Capacity management (scaling out solution as necessary)	Supplier
HDS	Ensure license compliance for HDS infrastructure	Supplier
HDS	Ensure license compliance for Customer applications deployed within HDS	Customer
HDS	Security / Functional Patching of the solution	Supplier
HDS	Agree to service outages	Customer
HDS	Be made aware of unplanned service outages / incidents	Customer
HDS	Inform users of service issues / changes	Customer
HDS	Manage changes	Customer
HDS	Manage incidents	Customer
HDS	Manage problems	Customer
Change Management		
HDS	Own the Gold build & ThinApp blue print	Customer
HDS	Own & operate the Gold build release process	Customer
HDS	Specify technical changes	Customer
HDS	Specify new ThinApps	Customer
HDS	Specify ThinApp changes	Customer
HDS	Specify new Gold build	Customer
HDS	Specify Gold build changes	Customer
HDS	On-board new organisations who wish to utilise the service	Customer
HDS	Approve technical changes	Customer

3) IMPLEMENTATION & ACCEPTANCE

3.1) PRESALES

Redcentric presales (both infrastructure and network) will work with the Customer to understand the requirements, scope the potential service options and document the solution. This will cover at least:

- Single or dual site solution
- Number of defined users, concurrent users, desktop types, workload, persistent / non-persistent required
- Amount of user and shared file stores
- Number of applications to be deployed on HDS, whether Gold image or ThinApp
- Network access methods and complementary services
- Addition of 2FA for user authentication
- Integration required to other Customer environments

3.2) CUSTOMER ON-BOARDING

Redcentric service delivery (project management, infrastructure and network engineering) will work with the Customer to setup and test HDS. This will cover at least:

- Provision of HDS, including design, delivery and systems acceptance testing
- Delivery of 5 Customer applications, covering Gold image and ThinApp
- Create Redcentric configuration items relevant to HDS for the Customer

The target lead time to complete service delivery is detailed in the table below, for each service element. This is subject to the timescales of delivery of the specific connection mechanism used to connect the Customer to IaaS, such as delivery of Ethernet access circuits, NHS network (N3) connection, Internet address allocation via RIPE, firewall configuration, options selected, etc.

Service Element	Service Activation Timescales
HDS Implementation	Target completion within 60 working days

3.3) CUSTOMER OFF-BOARDING

Redcentric will perform the following off-boarding tasks on cancellation of HDS:

- Decommission the HDS service, including desktops and file shares
- Decommission supporting network services
- Decommission HDS specific configurations items in Redcentric's service management platform

3.4) IN-SERVICE CHANGES

HDS supports changes to the number of defined users, concurrent desktops, deployed applications, user and shared file stores during the life of the service. The Customer will make a configuration change, via Redcentric's support desk.

3.5) ACCEPTANCE

Redcentric will perform functional testing following on from HDS implementation. Upon completion of the functional testing, Redcentric will issue an acceptance form to the Customer. Redcentric will provide feedback forms to the Customer to complete as their testing progresses.

The Customer will perform user acceptance and performance testing for HDS.

The Customer will be responsible for performing functional testing required as part of a desktop update, whether deploying new applications (Gold Build or ThinApp) or Microsoft updates.

4) SERVICE LEVELS AND SERVICE CREDITS

4.1) SERVICE LEVELS

The Service Level applicable to HDS is as follows:

Service Level: Availability **Measurement Period: Month**	
Service Level for a single site HDS deployment	Not less than 99.00%
Service Level for a dual site HDS deployment	Not less than 99.99%

4.2) FLOOR SERVICE LEVEL

The Floor Service Level applicable to HDS in respect of Availability shall be 85% in any given Month.

4.3) SERVICE CREDITS

The Service Credits applicable to HDS shall be calculated as follows:

$$Service\ Credit = \frac{C\ x\ S}{MS}$$

Where:

- S = the number of seconds by which Redcentric fails to meet the Service Level for Availability in the relevant Month
- C = total Charges payable in respect of HDS for the same Month
- MS = the total number of seconds in the same month

5) DATA PROCESSING

5.1) DATA PROCESSING SCOPE

- For the HDS Redcentric is responsible for managing the desktop operating system and the HDS platform.
- Redcentric does not access, alter or use any application data that is running on the HDS Service except as specifically stated below.
- In terms of operating the HDS, commands are passed to VMWare and the Microsoft Desktop Operating System and associated supporting servers. It is Redcentric who issues these commands, but these commands are for managing the OS and HDS platform and are not processing data.
- Customer data that is stored on storage servers is not backed up as part of this Service – see 5.5 below.
- The HDS platform is backed-up by Redcentric as part of the management of the Service, but this does not include Customer data.

5.2) DATA STORAGE AND UNENCRYPTED DATA

- The data that is stored in the Nimble storage servers can be encrypted if the Customer chooses this option in the pre-sales process, and it is not possible for Redcentric to access encrypted data. It is technically possible for Redcentric to access unencrypted Customer data on the storage servers; however, in the course of normal operations Redcentric has no reason to, and will not, access this data except in the course of providing support, which will be at the request of and in conjunction with the Customer.
- In the course of normal operations, the platform generates operational data such as log files. Redcentric has access to this data because it has administrator rights to the HDS. This operational data does not contain Customer specific application data, including Personal Data.
- The HDS will be using local working memory to process application data, and Redcentric has access to this data because it has administrator rights to the HDS. In the course of normal operations Redcentric has no reason to, and will not, access this data except in the course of providing support, which will be at the request of and in conjunction with the Customer.

5.3) DATA PROCESSING DECISIONS

- In the normal course of business Redcentric does not make any data processing decisions in relation to the Service. Processing is automated and instigated by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4) SERVICE CONFIGURATION WITH RESPECT TO DATA

- The service configuration will be done by Redcentric as requested by the Customer.
- The service configuration does not involve Customer data.

5.5) DATA BACKUP

- No data is backed-up by or as part of this Service.
- If the Customer uses the Redcentric Managed Backup Service (MBS), then the Data Processing section (Section 5) of the MBS Service Definition applies; if the Customer does not use MBS, then no data is backed up by Redcentric (and the Customer is responsible for its own backup arrangements and all backed up data).

5.6) SUB-PROCESSORS

- No other parties are involved in delivering this service, and there are no sub-processors.

5.7) CUSTOMER ACCESS TO DATA

- The Customer has login rights to the HDS that enables it to access, copy, process and back up data as it wishes.

5.8) SECURITY ARRANGEMENTS AND OPTIONS

- The HDS servers are hosted at Redcentric's data centres with physical data centre security and cyber security measures (e.g. Firewall) in place to protect the back end systems and platforms.
- Customers have access via a portal to VMWare Horizon to manage the configuration of HDS so they could in theory interact directly with the back end systems to edit configurations. However this access is provided for the Customer to manage the Golden Image.
- User access to HDS utilises Microsoft Windows Active Directory (AD) authentication.
- 2-factor authentication (2FA) can be added to HDS, as a chargeable option, to improve the logon security and is used wherever access to secure environments, such as HSCN, is required.

5.9) SERVICE OPTIONS

- Customers have the option to take the Redcentric Managed Backup Service, in which case:
    - as part of that Service, Redcentric will manage the backup of Customer data; and
    - the Data Processing section (Section 5) of the Redcentric Managed Backup Service Definition applies.

HARROGATE (HEAD OFFICE)

Central House
Beckwith Knowle
Harrogate
HG3 1UG

THEALE

2 Commerce Park
Brunel Road
Theale
Reading
RG7 4AB

CAMBRIDGE

Newton House
Cambridge Business Park
Cowley Road
Cambridge
CB4 0WZ

READING

3-5 Worton Drive
Reading
RG2 0TG

LONDON

Lifeline House
80 Clifton Street
London
EC2A 4HB

HYDE

Unit B
SK14 Industrial Park
Broadway
Hyde
SK14 4QF

INDIA

606-611, 6th Floor
Manjeera Trinity Corporate
JNTU – Hitech City Road
Kukatpally, Hyderabad – 72

0800 983 2522
sayhello@redcentricplc.com
www.redcentricplc.com

redcentric
business technology. managed.

bsi.
ISO 9001 Quality Management FS 603185
ISO 22301 Business Continuity Management BCMS 603194
ISO/IEC 27001 Information Security Management IS 603187
ISO/IEC 20000-1 Information Technology Service Management ITMS 668453