Business Requirements Specification

UNISTAD
Khalifa Stadium

Base Services

2.2 Building Access Control Services &
2.10 Intruder Detection

Prepared for: Supreme Committee for Delivery & Legacy

Document Reference number: SC-I60-CAB-ORD-SPE-IT-00158

Prepared by: Ooredoo Q.P.S.C

Supreme Committee for Delivery & Legacy
PO BOX 62022, Al Bidda Tower, 34th Floor
Corniche Street, Dafna Area, Doha, Qatar

Please note:
UNCONTROLLED VERSION WHEN PRINTED OR SAVED LOCALLY
Refer to the Controlled Document in eP PM Portal for the latest version. Any suggestions/feedback on this document are to be emailed to dc@sc.qa

Approval sheet

Document owner: Muhammad Abdullah Rana ,PM Ooredoo

Signature:	Date: 16/08/2021

UNISTAD WO ref. number: WO-25 (KS.DG1)

Revision history

Revision	Date	Additions/modifications
0	15-Aug-2021	First issue

UNISTAD WO ref. number: WO-25 (KS.DG1)

		Title	Signature	Date
Prepared by	Muhammad Abdullah Rana I have prepared this document having identified SC requirements.	Ooredoo, Project Manager		16/8/2021
Consulted and Supported by	Balaji Sankararaj I have reviewed this document having identified SC requirements.	Supreme Committee, Lead Business Analyst		16 Aug 2021
Reviewed and Recommended by	Suraj Seshadri I have reviewed and recommended this document having identified SC requirements.	Supreme Committee, ICT Consultant	Suraj Seshadri	17 Aug 2021
Reviewed and Approved by	Hugh McCallum I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements.	Supreme Committee, FM Consultant		18 Aug 2021
Reviewed and Approved by	James Stearn I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements.	Supreme Committee, Security		19 Aug 21
Reviewed and Approved by	Captain Ahmad Al-Kubaisi I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements.	Program Manager, Safety and Security Operations Committee - TATU		29.8.2021

Glossary & Acronyms

Name/Position	Description
ACS	Access Control System
API	Application Programming Interface
CCTV	Close Circuit Television
COTS	Commercially Off The Shelf
CPU	Central Processing Unit
CSN	Card Serial Number
GUI	Graphical User Interface
HVM	Hostile Vehicle Mitigation
ID	Identification
IDS	Intruder Detection System
I/O	Input Output
MOI	Ministry Of Interior
MS	Microsoft
NCC	National Command Centre
OS	Operating System
PAB	Personal Attack Button
PIN	Personal Identification Number
SC	Supreme Committee
SCTC	Supreme Committee appointed technical contractor
SDK	Software Development Kit
SSOC	Safety and Security Operations Committee
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol and Internet Protocol
TDO	Technical Delivery Office
UID	Unique Identification Number
VMS	Video Management System
WYSIWYG	What You See Is What You Get
YMCKO	Yellow Magenta Cyan Black Overlay

Contents

1. Introduction

Building Access Control Services, from this point forward referred to as the System, is one of the most critical services of the stadium. The intended outcome of the System is to enable operators to control and monitor pedestrian and vehicle access into, and within, the stadium while detecting unauthorised access and raising a discrete alarm from those in distress

1.1 Purpose

The purpose of this Business Requirements Specification is to identify TDO and Security Committee requirements for the system, required immediately following handover by the stadium contractor, in order to inform design development and delivery by the UNISTAD/SCTC solution provider.

This document will be used as the basis for the development of high-level design, technical specifications, testing and commissioning plans, training plans and handover documentation.

1.2 Scope

The requirements contained herein represent the current minimum required at Khalifa International Stadium. The Building Access Control services also includes Intruder Detection System.

Intrusion detection services provides Break-in alarm capabilities which use different sensors, motion detection; seismic detection capabilities to detect and report unauthorized access in defined zones and locations. Solution will integrate with CCTV surveillance to provide visual monitoring in case of an alarm or intrusion.

Building Access Control System will be implemented as part of the stadium commissioning (Base Services) and these systems shall able to integrate with Unified Identity Management, UNISTAD etc. which will be implemented in later stage

It will be able to support different access control credentials such as RFID / Proximity cards and Biometric readers etc. and shall be capable of integrating with other systems considering future enhancement such as accreditation and has provision to manage and provide access based on roles and zones.

Intruders Detection Service provides Break-in alarm capabilities which uses different sensors, motion detection, seismic detection capabilities to track and report unauthorized access in defined zones and locations

Requirement Stakeholders are represented by the column head “Stakeholders” in the requirements tables as:

- TDO for SC-TDO Security;
- SSOC for Security Committee.

The document does not include any Tournament specific requirements.

1.3 Requirements

1.3.1 Stakeholders

1.3.1.1 Stakeholders

- TDO for SC-TDO Security;
- SSOC for Security Committee.

1.3.2 Functional Requirements

1.3.2.1 Strategic Requirements

No	Description	Stakeholder
FN 1.1	Restrict access to authorised persons and vehicles;	TDO, SSOC
FN 1.2	Facilitate the controlled entry and exit of personnel with legitimate access rights into restricted and controlled areas;	TDO, SSOC
FN 1.3	Deter, detect and delay attempts at unauthorised access;	TDO, SSOC
FN 1.4	Enable an authorised user to raise a discrete alarm while under duress;	TDO, SSOC
FN 1.5	Support security and search and screening in preventing the introduction of prohibited and restricted items, and the unauthorised removal of items and materials.	TDO, SSOC
FN 1.6	Operate 24/7 with a high level of resilience	TDO, SSOC
FN 1.9	The system shall satisfy the requirements through: • Provision of an integrated access control and intruder detection system;	TDO, SSOC
FN 1.10	The system shall satisfy the requirements through: • Providing flexibility, allowing future configurable use cases to be captured and implemented with minimal disruption following construction and hand-over to venue operations; and	TDO, SSOC
FN 1.11	The system shall satisfy the requirements through demonstrating compliance with: Security Design Guide Q22M-APW-CMN-PMC-STR-0790 Rev1; ICT Standards and Specifications Criteria for Sports Venues SC-160-CAF-TEC-STD-00001	TDO, SSOC

1.3.2.2 General

No	Description	Stakeholder
FN 2.1	In emergency situations, the ACS shall be able to automatically open access-controlled doors and gates (except high secure rooms).	TDO, SSOC
FN 2.2	The system shall provide a mustering function in combination with a dedicated muster credential readers and report printer, located at a predesignated 'safe' place.	TDO, SSOC
FN 2.3	Initiate events based on integration with different access control and intruder detection sensors. SDK and API will be shared for the integration.	TDO, SSOC
FN 2.4	Rapidly lock and unlock individual and predefined groups of doors/gates from security Workstation (HMI).	TDO, SSOC

1.3.2.3 User Interface

No	Description	Stakeholder
FN 3.1	Security operators shall perform system configuration, viewing, recording, archiving and retrieval of access logs from a single workstation, promoting increased operational efficiency, removing operational silos and reducing training costs;	TDO, SSOC
FN 3.2	-The System shall integrate ACS and IDS with the CCTV system to enable operators to view live and recorded video concurrently on a single platform used for access control and intruder detection.	TDO, SSOC
FN 3.3	The user interface shall be highly configurable and shall take the form of a defined screen layout of areas/facilities where the user will only have access to those areas/facilities, which are appropriate to their job functions.	TDO,SSOC
FN 3.4	The user interface shall be so designed as to facilitate, as fast as possible, operator interaction with the subsystems.	TDO,SSOC
FN 3.5	The design of the interface shall place the most frequent actions in an immediately available and easily accessible form so that the operator does not have to search for action objections relative to each specific task.	TDO,SSOC
FN 3.6	A fully dynamic multi-layer mapping/display solution fully synchronized with the event stack. Plotting of devices in the MAP Layout (AutoCAD, PDF, JPEG Formats)	TDO,SSOC
FN 3.7	Vertical drill down movement up and down map layers and horizontal movement between plans depicting the areas on the same layer.	TDO,SSOC
FN 3.8	The mapping system shall include dynamic and animated icons that shall change state in real time according to the status of the object which they represent. It shall be possible for any object within the system to be represented by an icon on the mapping system.	TDO,SSOC
FN 3.9	The system shall include a suite of premade icons, the ability to import icons and an integrated function or tool that shall allow the administrator to make their own icons	TDO,SSOC
FN 3.10	Icons shall be large enough to allow a user to easily select them. To avoid clustering icons in heavily populated map areas the maps shall be so arranged and layered to ensure that icons do not overlay one another, that selection of one icon amongst a group or cluster of icons is easy and can be executed without inadvertently selecting the wrong icon.	TDO,SSOC
FN 3.11	Icons shall include context sensitive right click menus to provide details of status or options, variables or properties of the object being represented.	TDO,SSOC
FN 3.12	Dynamic drill down on receipt of an alarm or event. This drill down shall present to the operator the map level that best shows the event location.	TDO,SSOC
FN 3.13	Access to the areas based on their scope of responsibility. Operation changes at one workstation (such as changes of map due to alarm) shall not be reflected at other workstations. Only the workstation of the operator handling the alarm shall bring the relevant mapping to the fore. Mapping configuration shall, however, allow workstations to be dedicated to specific areas of the building or site and in this arrangement only those maps for the area associated with the workstation shall be available to the operator logged in at the workstation.	TDO,SSOC

No	Description	Stakeholder
FN 3.14	The user interface shall host a database of users/operators with associated rights to make visible and grant or deny differing levels of access to each system function.	TDO,SSOC
FN 3.15	The mapping system shall include dynamic CCTV image presentation within/over the map. CCTV associated with alarms shall be presented in the CCTV pop up window.	TDO,SSOC
FN 3.16	All maps to have navigation controls and shall include: Return to the home page Move up and down one layer Move side to side on the same layer (where the site is depicted in tiles)	TDO,SSOC
FN 3.17	Maps and event stack (list) shall be fully synchronised. As an event appears in the event list it shall also cause the respective icon (where assigned) to indicate the change of state on the mapping system without any perceivable delay. Similarly, if an event is acknowledged and cleared through interaction with the representative map icon then the new status shall immediately be reflected in the event list.	TDO,SSOC
FN 3.18	All software (applications, services, drivers and other software) required for a product, device or system to work shall automatically start without user intervention and shall not require a user to be logged in to the hosting computer or to actively start the application.	TDO,SSOC
FN 3.19	All software shall be designed to work with the operating system selected by the software author without fault or interruption, shall be wholly compatible with the selected operating system and shall include full error trapping and handling routines such that any faults or errors that may occur present to an operator or present a message that is in an understandable and meaningful format to a lay person.	TDO,SSOC

1.3.2.4 Access Rights

No	Description	Stakeholder
FN 4.1	Users of the CCTV and ACS and IDS shall include single login with a fully integrated security context.	TDO,SSOC
FN 4.2	The user shall automatically be logged out following a period of system inactivity. The period of inactivity shall also be configurable according to the requirement.	TDO,SSOC
FN 4.3	Security operators shall perform system configuration, viewing, recording, archiving and retrieval of access control and intruder detection transactions from a single ACS workstation, promoting increased operational efficiency, removing operational silos and reducing training costs.	TDO,SSOC
FN 4.4	System configuration and diagnostics capability to set and maintain the configuration of ACS and IDS hardware (e.g. database servers, camera servers, etc.) and administer operators with permissions, priority levels, etc. (where appropriate);	TDO,SSOC

No	Description	Stakeholder
FN 4.5	The workstation GUI shall be the interface through which the operators carry out the day to day access control and intruder detection system monitoring and control;	TDO,SSOC
FN 4.6	Time and date stamped audit trail of all ACS and IDS transactions, camera displays, operator actions and system performance;	TDO,SSOC
FN 4.7	The system shall require all users to log on and shall record all actions of the user while logged on.	TDO,SSOC
FN 4.8	The system shall enable each building to be logically partitioned into separate locations and their associated cardholders logically partitioned into separate organizations.	TDO,SSOC
FN 4.9	Each location/organization shall have a logical set of access points, cardholders, cards, reports, and displays.	TDO,SSOC
FN 4.10	Access to cameras and components in the ACS and IDS shall be restricted based on an area or facility (stadium) security model. Each ACS and IDS device will be assigned to an area or facility. A user authorised to view a particular area or facility can access any resource assigned to that area or facility. A user shall not be aware of, and unable to access, ACS and IDS devices assigned to an area or facility that they are not authorised to view.	TDO,SSOC
FN 4.11	Access shall be gained to the Windows operating system by logging onto the computer using a user account name and password. This is true for both local and remote terminal services access. Because user accounts may be well known or easily guessed within an organization, the password becomes the prime vehicle for authentication. User account and password policies are therefore important security measures.	TDO,SSOC
FN 4.12	The system operator accounts shall be set up with individual accounts for each operator	TDO,SSOC

1.3.2.5 Reports

No	Description	Stakeholder
FN 5.1	The system shall provide a simple and flexible way to extract information from the server database available in ACS and IDS.	TDO,SSOC
FN 5.2	The system shall enable fully flexible database reporting with the ability to generate reports based on one or more and any combination of fields in any database table linked to any number of other tables and based on one or more and any combination of fields in any other database. Only those fields included in the report structure shall be output.	TDO,SSOC
FN 5.3	The system shall have ability to export the output of any report, whether based on a template or user definition as a data subset in .txt, .csv, .xls or any other common export format including second normal form (2NF).	TDO,SSOC
FN 5.4	A viewer or reader shall be installed to allow the report to be read as exported.	TDO,SSOC
FN 5.5	The ability to print to PDF, to include provision of a PDF driver on all servers and on all workstations.	TDO,SSOC

No	Description	Stakeholder
FN 5.6	The ability to save or export the results of a report either within the system as a report or externally to the system as an exportable report file that can be distributed for reading without the native application used for creation.	TDO,SSOC
FN 5.7	The ability to create and save (for future use) custom report templates.	TDO,SSOC
FN 5.8	The system shall provide functions whereby reports can be based on multiple "and", "not" and similar logical operators, including multiple levels of nested operators.	TDO,SSOC
FN 5.9	Export to another program format (such as Microsoft Excel), shall either not require the native programme or shall include all external reference files, applications and resources required	TDO,SSOC
FN 5.9.1	The following table identifies the report types – to be filled RPT1: Alarm/Event This Sample reports lists a summary of alarms and events by location and by date and time. It includes a graphic summary.	TDO,SSOC
FN 5.9.2	RPT2: Cardholder List Lists card details for cards corresponding to specified search criteria based on any cardholder field.	TDO,SSOC
FN 5.9.3	RPT3: Present in Zone Lists all cardholders present in defined zone. Useful for auditing and mustering.	TDO,SSOC
FN 5.9.4	RPT4: Unused Cards Lists cards that have not accessed any door or zone within defined date / time range	TDO,SSOC
FN 5.9.5	RPFT5: Mustering An exception list of all persons who are known to have been in the building at the time of the evacuation event but who have not logged their presence in the safe area through presentation of their credential the one of the designated muster card readers	TDO,SSOC

1.3.2.6 Enrolment

No	Description	Stakeholder
FN 6.1	The system shall support pre-registration to include • Security level; • Access areas/zones; • Length of stay / validity period; and • Maximum number of entries	TDO,SSOC
FN 6.2	The system shall support Group / Event pre-registration, pre-loading of visitor photos, badge pre-printing and arrival instructions	TDO,SSOC

No	Description	Stakeholder
FN 6.3	The system shall include all associated hardware, software and peripherals in order to capture and process visitor information, including but not limited to • Qatar ID; • Driver's License; • Passport; • Photograph; • Business cards.	TDO,SSOC
FN 6.4	Following pre-registration, the system shall complete visitor registration within 15 seconds per visitor; registration of permanent staff may be extended as a consequence of additional processes	TDO, SSOC
FN 6.5	Visitors that do not show shall be automatically removed from the pre-registered list at the end of the visit period	TDO, SSOC

FN 6.6	The system shall include a fully integrated Photo ID card design and production system providing the following features • WYSIWYG layout of design; • Dynamic links to the underlying database to allow any field in the database to be displayed on the card; • The software shall include the ability to deal with head and shoulders images of card holders and shall include native capture mechanisms including the import from a file of any industry standard computer graphics format, scanners and video grabber/capture cards; • The software shall include the ability to deal with signatures of card holders and the system shall include native capture mechanisms including the import from a file of any industry standards computer graphics format, scanners, drawing tablets, electronic signature pads and video grabber/capture cards; • Images shall be captured through the software within the underlying database as opposed to systems that store image files external to the database as individual files or within another database; • The software shall include a full suite of design tools to allow the creation of backgrounds and display artefacts such as squares, rectangles, circles and triangles and shall include the ability to choose any system colour and differing levels of opacity for any individual object; • The software shall include tools to layer objects, to send objects in front of and behind other objects and to merge objects together to create complex non-standard shapes; • The photo ID suite hardware shall take the form of an analogue video capture card with an attached analogue camera or an IP based camera with a suitable manual zoom varifocal lens mounted on a tripod capable of being floor or desk mounted; • The system shall create high colour, head and shoulder views of subjects of sufficient quality to be incorporated into a badge design. Suitable shadow free subject target lighting shall be provided, assuming a room environment with lighting of 300Lux or less; • Printing of cards shall be to a single sided dye sublimation printer with YMCKO dye films and shall provide not be less than 300 cards per film. The printer, two new print rolls and one cleaning kit shall be supplied. This shall be in addition to any existing print panel that may be partially used for testing, demonstrations or testing, the remaining portion of which shall be left on site; • The printer shall support reverse side printing (not double sided printing) with monochrome/overlay only prints. Any combination of front or back, colour, mono printing shall be supported according to what type of ribbon is installed in the printer; • Two card printers shall each include not less than a 50-card input and a 50 card output hopper and shall have both a USB and an Ethernet interface. Wireless interfaces may not be provided. Print speed shall be no more than 25 seconds per card side in colour and no more than 10 seconds per card in monochrome; • The system shall use Mifare DESFire cards and the card printers shall therefore include compatible Mifare card encoders;	TDO,SSOC

No	Description	Stakeholder
	• The system shall include a signature capture tablet to obtain highly accurate signature images. The image shall be stored as a template within the database	
FN 6.7	The system shall support multiple enrolment readers, the purpose of which shall be to automatically decrypt, read and enter the number of a card being presented for the purpose of either validation or for automatically entering the card value into the card number field on the card entry form.	TDO,SSOC
FN 6.8	The system shall support fast processing of large groups of visitors through queuing of captured data	TDO,SSOC
FN 6.9	Two enrolment readers shall be installed alongside two photo ID units. The enrolment reader shall take the form of a reader mounted on or in an enclosure that shall include all necessary power and connections. The enclosure shall be suitably selected and the installation designed for use as a free standing desk mounted device	TDO,SSOC
FN 6.10	The system shall provide quick, cost-effective and individualized card as an essential component of effective person identification. The system shall allow for printing of individualised visitor card containing the following as a minimum • Name; • Photograph; • Expiration date; • Valid access areas.	TDO,SSOC
FN 6.11	The system shall support customised card templates for: Staff, Visitors, VIPs, Contractors and any other user groups.	TDO,SSOC
FN 6.12	The system shall support a pre-print functionality which enables a process that shall automatically pre-print cards for expected visitors before they arrive. The user shall be able to configure pre-printing for a specific company and access area.	TDO,SSOC
FN 6.13	The system shall support the printing of colour cards on 4” by 6” fold-up, clip-ready, tamper-resistant stock.	TDO,SSOC
FN 6.14	The system shall support printing of cards on • Thermal label printers: Dymo 330 and 330 Turbo – thermal paper labels or equal and approved • Dye Sublimation – PVC cards • Ink / Laser printer – Regular card stock	TDO,SSOC
FN 6.15	The system shall support operators authenticating a person as having proper identification and determining that he or she is who they claim to be by recalling of individuals previously registered on the system, including their photographs	TDO,SSOC
FN 6.16	Unwanted guests, ranging from disgruntled ex-employees to known undesirables, shall be capable of being imported into a Watch List, including cross matching for alias names, to alert personnel of a potential threat.	TDO,SSOC
FN 6.17	The system shall check each registered individual against the host employee’s personal pre-authorized and denied list, including a Watch List of barred individuals. The Watch List shall provide viewing of picture and person’s attributes, reason for being on the Watch List, and action to perform upon arrival	TDO,SSOC

1.3.2.7 Credential Management

No	Description	Stakeholder
FN 7.1	Support multiple access control credential types including but not limited to • non-contact passive credentials with readers; • integrated combined card readers with PIN pads; • integrated combined card readers with biometric readers; and • any other credential type that may form part of event related accreditation.	TDO,SSOC
FN 7.2	The system shall incorporate an arrangement where the requirement to enter a PIN in order to gain access can be switched on or off according to a time schedule or other system event. For example, the PIN shall be required to be entered between 00:00 and 07:30 not required between 07:30 and 09:30 required between 09:30 and 16:30, not required between 16:30 and 18:30 and required between 18:30 and 00:00. Furthermore, also as an example, the PIN requirement can be overridden by a system mode so, depending on the mode, the mode shall override the systems setting to automatically raise the level of security (i.e. shall change the system settings from no PIN required to PIN required	TDO,SSOC
FN 7.3	The system shall also support a configuration where the PIN component is all that is required for access to be granted. In this mode the reader element is disabled – the same examples of time schedules shall enable or disable this function as shall mode changes override the configuration	TDO,SSOC
FN 7.4	Card credentials shall double as photo ID providing a visual method of identifying card holders around the buildings as they shall carry a photograph of the holder	TDO,SSOC
FN 7.5	Authorize access based on any combination of the following individual or groups of: • Cards; • roles; • doors, areas/zones; and • time/dates.	TDO,SSOC
FN 7.6	Track and report unauthorized access for specified users, roles, doors, areas/zones and times/dates.	TDO,SSOC
FN 7.7	Individual programming by card credential so that some cards shall be able to access doors while other cards shall not.	TDO,SSOC
FN 7.8	In addition to the standard properties such as access rights and time zones the system shall support the following user/credential modes :	TDO,SSOC
FN 7.8.1	Supervisor Only credentials designated as ‘Supervisor’ shall operate the supervisor mode. In supervisor mode multiple presentation (not less than 3) of the credential in quick succession (typically within a time frame of not more than 2500ms) shall cause an event to occur. For example, a supervisor designated credential used at any door shall cause the door to enter bolt status. Individual doors/readers can have different supervisor mode responses configured. At these points activation of the supervisor mode shall enact the specific response programmed for the event	TDO,SSOC

No	Description	Stakeholder
FN 7.8.2	Dual Release In Dual Release mode two credentials, both with appropriate access rights, shall be presented to the reader in order for the door unlock/release to occur	TDO,SSOC
FN 7.8.3	Stand back Stand back mode is predominantly used for visitors. To ensure the visitor is always under escort. Stand back mode creates a temporary one-shot change to a visitor's access rights for a given door. In Stand back mode the visitor credential shall be paired with the host credential. The visitor credential shall have only limited access rights. The host credential, when used at a door where the visitor shall not have access rights allows the host to enter from the insecure side to the secure side and in so doing temporary access is granted to the visitor to pass through the same portal. The host, now on the secure side, is able to receive the visitor into the secure side of the door where the visitor uses their credential in order to gain one-time access. Once the visitor has used their credential at the door the temporary access rights are removed from the visitor's credential	TDO,SSOC
FN 7.8.4	Mobility Impaired (MI) Open The system shall support designation of an extended opening time for mobility impaired use.	TDO,SSOC
FN 7.8.5	Extend Open The system shall provide variable extended opening times for technicians, facility management staff and other users who shall have an extended opening to avoid causing nuisance alarms.	TDO,SSOC
FN 7.8.6	Guard Guard mode shall allow a security guard to validate a user and then permit the user to enter. In guard mode the guard shall present both their own credential and that of the user to the reader system – both events are recorded, and the user is permitted entry. Guard mode operates only at readers designated for the purpose	TDO,SSOC
FN 7.8.7	Holiday The system shall support holiday schedules. In a holiday schedule the user's credential shall not allow access to any area during the holiday. The system shall support national holidays as well as personal holiday schedules. Credentials shall not work within holiday periods unless explicitly exempted from the specific holiday day. The holiday schedule ends five (5) minutes before the credential holder is due to return to work (and not just at the commencement of the day (typically 00:00:01). Thus, if the credential holder is due to return to work at 09:00 on the 1st of January the schedule shall enable to credential at 08:55 on the 1st of January and NOT at 00:00:01 on the 1st of January	TDO,SSOC

No	Description	Stakeholder
FN 7.8.8	Holiday Exempt Credentials can be designated holiday exempt. This function shall be programmable linked with Holiday modes. If a card holder is designated as holiday exempt they can be exempted; i.e. allowed into the building, on a public holiday as they would in fact be working. The exemption shall be applied to the specific public holiday that they are required to work on. Exemption does not apply to all public holidays. Exemption shall be set prior to each public holiday for the specific holiday to be exempted from. Holiday exempt does not override private holiday periods	TDO,SSOC
FN 7.8.9	Suspension Period A value in days commencing from the last full access, configurable per card within which the credential shall be used to permit continued full access. The credential shall be automatically suspended if the credential has not been used within the suspension time. For example, a card with a 10-day suspension time period is used on the second day of a month. If the card is then not used for 10 days, the card shall become automatically suspended and shall not allow access if used on the 13th day or beyond until the suspension is lifted by a duly authorized operator	TDO,SSOC
FN 7.8.10	Temporary The system shall support automated credential management. A credential designated “temporary” shall remain active only until the end of the day of issue when it shall be automatically suspended. Any card not used in the system (i.e. not associated with a full entry event) within a defined period of time shall be automatically suspended	TDO,SSOC
FN 7.8.11	Purge The system shall support purging of credentials. The purge event shall cause all cards not successfully used within a user configurable time period (which shall be less than the suspension period) to be automatically suspended. The purge event can be linked with threat level changes, with a physical input (or input group) change of state or with a time schedule	TDO,SSOC
FN 7.8.12	Duress The system shall provide a duress facility initiation through a form of alternative credential use that is not obvious to the person causing the state of duress to the system user	TDO,SSOC

No	Description	Stakeholder
FN 7.9	The system shall support multiple statuses but a credential can only have a single status at any one time • Blocked: A card is blocked for a temporary, specific period (day, week, month, etc.). • Void: A card void is indefinite but can be un-voided through manual intervention by an operator. • Suspended: The suspended card follows an automated event (not available to an operator). The card can be reinstated. • Annulled: The annulled credential is permanently disabled from working at any portal or doors. The annulled status cannot be reversed. Any credential set to annul cannot be reused in its as annulled state and shall either be reprogrammed or replaced. However, while an annulled credential shall not release any portal or door any attempt to use an annulled credential shall be recorded to the system database and shall generate a high priority alarm event. • Deleted: Credentials cannot be deleted once enrolled on the system. There shall be no delete function. The equivalent alternative to delete is 'annul'	TDO,SSOC

1.3.2.8 Dynamic Operating States and Crisis Management

No	Description	Stakeholder
FN 8.1	The ACS is to include multiple dynamic operating states (theoretically unlimited but allowance for at least 10). In the event of a crisis (such as an evacuation) or change of operational event (such as the arrival of an international dignitary) the system shall switch to a different operating mode, overriding time schedules and changing door locking profiles, event monitoring, user access rights and other operating parameters without being perceived.	TDO,SSOC
FN 8.2	Change of state to be on a time schedule or by operator command, the latter being either a menu selection or through a virtual on screen object (button).	TDO,SSOC
FN 8.3	Rapid (single button), concurrent 'lockdown' of all access points in a predefined group and removal of all access permissions except for a predefined privileged group.	TDO,SSOC
FN 8.4	Provide password protection for the change of an operating state from either a lower state to a higher state (in the case of rapid lock-down) or from a higher state to a lower state (allow for the option of different passwords).	TDO,SSOC
FN 8.5	The system shall support an unlimited number of time schedules for the automated activation and deactivation of system events and functions.	TDO,SSOC
FN 8.6	There shall be no actual limit to the number of schedules that can be created and no limit to the number of changes (on/off events) within a schedule. Although theoretical the system shall be capable of handling a time schedule that contains a full week of on/off events each delineated by one second (i.e. 1800 on events and 1800 off events per hour).	TDO,SSOC

No	Description	Stakeholder
FN 8.7	Activation of any break glass unit shall cause a door forced alarm event to be enunciated at the ACS Workstations. Each break glass shall be separately identified within the system by an individual alarm input for each device.	TDO,SSOC
FN 8.8	Activation of any panic alert button (PAB) shall cause an alarm event to be enunciated at the ACS Workstations. Each device shall be separately identified within the system by an individual alarm input for each device	TDO,SSOC

1.3.2.9 Event Management

No	Description	Stakeholder
FN 9.1	Events represent all ACS and IDS activity including benign and alarm events, debug events and every change of state of the system and its edge devices. Specific subsets of 'events' include: • Alerts: Lower priority activities that require the user/operators to analyse the events and determine if further action is required; • Alarms: Higher priority event indicating a serious event that needs prompt operator action. All alarms shall require alarm acknowledgement (the operator shall acknowledge receipt of the alarm) and clearing (the alarms will be cleared automatically once actions are completed).	TDO,SSOC
FN 9.2	All system and subsystem activity including alarm and every change of state of the system shall be logged as alert or alarm based on the priority/severity	TDO,SSOC
FN 9.3	It shall be possible for the user/operator to initiate an event. Initiating an event shall cause the system to record, as a minimum • The date and time of creating the record; • The machine name from which the record has been created; • The name of the user logged in at the machine; • A dialogue for entering the date and time of the incident (with radio boxes for recent time periods such as "one minute ago" "three minutes ago" etc. – use of the radio buttons shall automatically enter the system time less the radio button value); and • A dialogue for entering the event details	TDO,SSOC
FN 9.4	The dialogue for entering the event time shall be mandatory and modal. The dialogue for entering the event details shall be optional at the time of creating the entry. However, creating the entry shall result in an unacknowledged event. In a fast moving live monitoring situation the operator shall return to the data entry point and enter the event details together with other details on event closure once the event is ended.	TDO,SSOC
FN 9.5	The system shall support event types or groups. Event types or groups are a template to which events are assigned. Upon assignment of an event to an event type, the event inherits the properties defined by the event template. Actions can be assigned to an event template. Actions are then inherited by, and globally apply to, events allocated to the event type or group.	TDO,SSOC

No	Description	Stakeholder
FN 9.6	All events are recorded in the systems database, timed and dated (to not less than millisecond accuracy), fully indexed and searchable	TDO,SSOC
FN 9.7	All actions (including embedded system actions, regardless of status or severity) executed against an event, including automated or embedded system actions, shall be recorded in the database to include the following: • Field generated alarms and events; • The action (all user activity, to include details of any record changes, including the pre change value); • The action originator (the user name) and the machine name from which the action takes place; • The date and time of the action to millisecond time precision; • The event stack shall display events in text format scrolling up and down the computer screen displayed as a list.	TDO,SSOC
FN 9.8	The system shall provide an event stack, taking the form of a list of events, displayed in text format as a list scrolling vertically on the screen, presented to the operator for review, action.	TDO,SSOC
FN 9.9	The event list shall show all events from within the system and from all connected subsystems according to the default filtering applied according to the user log in or workstation configuration.	TDO,SSOC
FN 9.10	The ACS shall support multiple lists per user/operator. For example, the ACS shall support a list for high priority alarms and a separate list for events. The lists shall follow the user/operator and shall be applied to whichever workstation the user/operator is logged in at.	TDO,SSOC
FN 9.11	All alarms shall be assigned a priority and not less than 99 priorities shall be provided. The highest priority shall be 1. Alarms with higher priorities shall require enforced operator handling.	TDO,SSOC
FN 9.12	Priorities shall dictate the order in which events are to be displayed, automated actions initiated and user actions required. Under normal conditions the list shall be sorted by event priority. Events shall be displayed, sorted in descending order (highest priority first and at the top of the event list) with a secondary sort by date and time of event sorted in ascending order (oldest first).	TDO,SSOC
FN 9.13	The system shall include administration level configuration of the default entry sorting. Administration configuration of the default sort order shall be persistent and become “the default” sort order.	TDO,SSOC
FN 9.14	It shall be possible to display the list at machine level with differing permissions. This list shall automatically be presented when the computer starts and shall display the events programmed to be directed to it. There shall be controlled access to the formatting of the list that is configurable by the system administrator to include, but not be limited to, restrictions on actions and sorting or filtering	TDO,SSOC

No	Description	Stakeholder
FN 9.15	The operator shall be able to sort and filter the list dynamically. However, any dynamic sorting or filtering shall be non-persistent and shall be removed and reverted to default • After a predetermined and configurable time delay; • After log out of an operator; and • Any manual or applied sorting or filtering of the display shall automatically be overridden when an event is received that is of a higher priority than the priority of the highest event extant in the list at the time of receipt.	TDO,SSOC
FN 9.16	Any defined sort order shall not be persistent on log off/on. On log on the default sort order (sorted by priority, highest first, or as specifically configured by the administrator) shall be applied.	TDO,SSOC
FN 9.17	The fonts, point size and font properties, font and background colours and the visual scaling of the list together with which data columns are displayed in the list shall be configurable.	TDO,SSOC
FN 9.18	The list shall include dynamic functions including right click and double click functions to allow any system events relative to the displayed event to be enacted	TDO,SSOC

1.3.2.10 Event Monitoring

No	Description	Stakeholder
FN 10.1	The system shall provide the ability to trace the use of any card at any single, multiple or group of doors.	TDO,SSOC
FN 10.2	Trace shall be enabled according to password control to any one card. Only certain operators can enable trace to a card and only certain operators (not necessarily the same operators can activate or deactivate the trace function). Trace can be enabled/disabled against a time zone.	TDO,SSOC
FN 10.3	When enabled, trace shall display as a pop-up window or event in the event stack. The display can be activated at specific workstations, to specific user log-ins or any combination thereof.	TDO,SSOC
FN 10.4	The system shall allow reporting of cardholders who have the trace feature enabled with a separate report showing those cards where the trace is active. Access to the reports shall be password controlled. Persons who do not have access to the reports shall not be able to see that the reports exist.	TDO,SSOC
FN 10.5	Stealth mode shall be provided. This shall hide the card activity from the operator event screens but records events in the system database	TDO,SSOC

No	Description	Stakeholder
FN 10.6	The system shall provide a facility where specific doors can be designated as trace doors. This feature shall function in conjunction with the credential trace function. A door (portal) or doors (portals) as a group shall be set as trace points. Used in conjunction with the trace property, when enabled, a trace event shall occur: • When any card is used at a trace door; • Only when a trace card is used at a trace door. This differs from the credential trace property which is where the trace card shall create the trace event when used anywhere in the system.	TDO,SSOC
FN 10.7	Door monitoring shall provide live, real time monitoring including • Reader connectivity; • Reader tamper; • Door position monitoring; • Lock status (locked or unlocked) monitoring; • Request To Exit; • Box tamper; • Mains fail; • Low battery.	TDO,SSOC
FN 10.8	Door monitoring shall provide live, real time monitoring. Door Forced-Open and Door Held-Open events will be provided based on door position and lock status monitoring.	TDO,SSOC
FN 10.9	Positive indication mains status monitoring shall be included for each item of equipment on the field side of the access control system to include door control and locking and hardware in the communications path.	TDO,SSOC
FN 10.10	All doors/portals shall include both door position and lock status monitoring. Door and lock monitoring are not the same. There are conditions between door position and lock status that are largely mutually exclusive and require an alert to be given to the operators if they occur.	TDO,SSOC
FN 10.11	The system shall incorporate a mechanism whereby any alarm inputs that physically remain in the alarm condition after the alarm is processed at the user/operator workstation either: • Immediately resends the alarm status or prevents processing; and / or • Changes the status at the user/operator workstation	TDO,SSOC
FN 10.12	A condition where a physical or logical input is in an alarm condition but where the alarm condition is not actively displayed to the user on the user/operator workstation shall not exist	TDO,SSOC
FN 10.13	Door status shall also be listed as either: • Online; • Normal; • Event (Alarm / Alert); • Offline; • Deactivated (for maintenance); • Disabled (not used).	TDO,SSOC

No	Description	Stakeholder
FN 10.14	The system shall have capability to provide anti-pass-back facility. Anti-pass-back is a mechanism where a user cannot use their credential to conduct consecutive movements in the same direction through any portal. Therefore, each in transaction is followed by an out transaction and each out transaction shall be followed by an in transaction. A violation occurs if an “in” transaction is followed by another “in” transaction on unlimited specified doors within a specified period of time.	TDO,SSOC
FN 10.15	The system shall provide the capability to enrol temporary employees with automatic inactivation after a predetermined period of time. This shall allow, for example, contractors to act as hosts for other visitors while working on site for a certain period of time.	TDO,SSOC
FN 10.16	The system shall keep an accurate log by automatically tracking events as they relate to the visitor’s activities on site. The system shall track visitor sign in and sign out	TDO,SSOC

1.3.2.11 Event Response

No	Description	Stakeholder
FN 11.1	For events that require user/operator evaluation and potential further action, the system shall allocate the events to the user/operator preassigned to that area/facility, or to the user/operator when it is first acknowledged to that area/facility. Once an event has been acknowledged the system shall not permit any form of un-acknowledgement or assignment to null however the system shall allow the event to be reallocated to another user/operator	TDO,SSOC
FN 11.2	The system shall support a process of event handling based on the following logic order: • Event acknowledge (accept); • Execute associated actions; • Close event.	TDO,SSOC
FN 11.3	The system shall support “time to acknowledge” periods definable by specific event point or event group and the event shall be acknowledged within a defined period of time starting from the time (second) the alarm is received by the system. Failure to acknowledge within the time window shall escalate the event priority and shall be recorded in the system’s historical record. The reporting system shall allow reports on overall numbers of failures and to an individual operator level.	TDO,SSOC
FN 11.4	The system shall support both single level and dual level event interaction as well as events requiring no operator interaction. Events that require no interaction shall generally either not be displayed on the user screen (but will be recorded in the event database/table) or shall be displayed only for a period of time before being automatically removed from view.	TDO,SSOC
FN 11.5	For notification events or events that require no action, the event (or event group) may be configured to not require an operator closure action.	TDO,SSOC
FN 11.6	For single level event control, the operator will acknowledge the event through the use interface and in so doing the event will automatically closed.	TDO,SSOC

No	Description	Stakeholder
FN 11.7	For dual level event control, and upon receipt of an event, the user/operator is required to acknowledge or accept the event. The event remains active until closed. The user/operator is required to close the event after actions relative to the event are conducted. The event cannot be closed unless it has been accepted.	TDO,SSOC
FN 11.8	For partial closure, and events where a number of actions are associated, the system shall allow partial closure of the event where critical actions are complete but less important actions remain outstanding. Events that are partially closed take on a lower priority but will remain outstanding until all actions are completed	TDO,SSOC
FN 11.9	The system shall include a dual closure function, configurable for each event, that requires two different users/operators logged on separately, individually and at different workstations to close an alarm. The following two levels shall be provided • Standard: shall require two operators of any level to close the event; • Enhanced: shall require an operator, of a higher level than the operator who acknowledged the alarm, to close the event unless the operator who acknowledged the alarm holds the highest authority within the system in which case the operator who closes the event shall have rights to the same level.	TDO,SSOC
FN 11.10	Any alarm or event can be assigned to be closed by a single operator or only by two operators with a sub property to allow standard or enhanced closure as defined above.	TDO,SSOC
FN 11.11	The system shall enable events to be redirected. Events shall be directed to one or more or any group or combination of user workstations and to one or more users/operators. The higher redirect level takes priority so if a user/operator logs on to a workstation of an overall lower status the user/operator's log-in shall override the machine status.	TDO,SSOC
FN 11.12	The system shall enable any event to be assigned one or more and any combination of external notifications. External notifications shall include, but not be limited to personal e-mails, text messages, pager messaging, PMR notifications (by pre-recorded or digitized messages), etc. Notifications shall include the ability to allocate a group message or a specific message. Each event can be assigned more than one message addressed to more than one recipient. E-mail notifications shall include the ability to set up an automated notification of receipt by the recipient. In this case the source system sending the notification shall send an alert if the acknowledgement is not received within a user definable time window	TDO,SSOC

1.3.3 Non Functional Requirements

1.3.3.1 Performance & Capacity Requirements

Resilience

No	Description	Stakeholder
PCR 1.1	System availability shall not be less than 99.999% (five nines) available as measured across a rolling 12 month period, for the whole system, providing the full service, including but not limited to all transmission nodes, video management servers, storage, workstations and cameras.	TDO,SSOC
PCR 1.2	Minimise the effects of single points of failure on the overall surveillance capability while providing an integrated GUI such that operators are unaware of the redundant system configuration;	TDO,SSOC
PCR 1.3	Redundancy at the server and storage level to ensure full uptime availability. ACS Servers with N:1 Redundancy;	TDO,SSOC
PCR 1.4	The ACS system shall be available with two servers; one is dedicated as the primary server and the other acts as hot standby server Redundancy to include "hot standby" Access Control server and Database management system enabling mirrored servers to work in a single unified operating environment. A virtual availability manager shall run and monitor both physical servers and shall provide the pathway onto the appropriate IT Network. The availability management system shall meet the following requirements as a minimum; • Fault tolerant and provide 24/7 availability; • The management system shall be scalable to meet the needs of the system in terms of size and requirements, including immediately available and expansion capabilities; • A single server failure shall not impact on the system operation; • The management system and server switching shall be fully automatic in operation requiring no manual intervention; • Zero downtime while a server is either offline, during replacement or whilst the replaced server's system image is being rebuilt; • Authorised personnel automatically alerted of any actual or potential system failure through the network management system.	TDO,SSOC
PCR 1.5	Over and above these listed requirements, each server shall have in-built resilience by way of dual hard drives storing mirrored data and dual, hot-swap power supplies	TDO,SSOC
PCR 1.6	A watchdog built into each server shall constantly monitor the health of its hardware and alert authorised personnel of any actual or potential failure through the network management system.	TDO,SSOC
PCR 1.7	The power source shall be dual in each server to avoid the power failures. Disruption shall thus be minimized and recordings and live view shall be maintained without the need for manual cable swapping or hardware replacement.	TDO,SSOC

Scalability

The system shall be scalable to enable any unlimited number, size or capacity of the following without adverse impact on functionality or performance:

No	Description	Stakeholder
PCR 2.1	Additional access points (card readers, door controllers);	TDO,SSOC
PCR 2.2	Additional intruder detection sensors;	TDO,SSOC
PCR 2.3	Additional ACS/IDS workstations; and	TDO,SSOC
PCR 2.4	Additional servers and storage.	TDO,SSOC

General

No	Description	Stakeholder
PCR 3.1	Open Standard ACS and IDS	TDO,SSOC
PCR 3.2	ACS and IDS supports COTS (Commercially Off the Shelf) hardware for storage & server platforms; and	TDO,SSOC
PCR 3.3	ACS and IDS supports future enhancement of the edge devices (card readers, sensors), server, storage, power and network	TDO,SSOC
PCR 3.4	MIFARE DESFire EV1 cards with 4KB memory shall be used operating at 13.56MHz with a programme-wide 32bit UID (CSN) read as ISO decimal format	TDO,SSOC
PCR 3.5	Under no circumstances shall the UID (CSN) be used to authenticate the validity of the credential for the purpose of control of access to secure areas, other than to initiate introductory or preliminary data exchanges	TDO,SSOC
PCR 3.6	AES128 encryption on the OSDP connection	TDO,SSOC
PCR 3.7	It shall not be possible to clone the credential, nor shall it be possible to extract any of the data or application details from the card without due authorisation	TDO,SSOC
PCR 3.8	Up to 25,000 cardholders with unlimited access levels	TDO,SSOC
PCR 3.9	A fully on-line system residing on the Building Data Network and using Internet Protocol	TDO,SSOC
PCR 3.10	Door control hardware shall include the inherent facility to work offline, in independent mode, without degradation of performance or security provision. It is accepted that a controller designed to normally be online cannot operate offline indefinitely without some adverse effects, but these shall be limited to the overwriting of historical and alarm events and similar occurrences that do not affect the security afforded by the door controller. Door controllers which drop offline shall initiate a local audible door alarm monitoring and sent to the ACS monitoring system. The Contractor shall advise the SC of any limitations of the door controller when operating in offline mode	TDO,SSOC
PCR 3.11	In case of communication failure between the Access Multi Controllers and Access Control System software, Controllers will work in standalone and store all transactions in the controller. Once the communication link is restored all transactions (data/logs) stored in the controllers will be pushed back to the software.	TDO,SSOC

Integration

No	Description	Stakeholder
PCR 4.1	The system shall be fully integrated with other systems as required to enable the following: Control and monitoring of the electronic key management system;	TDO,SSOC
PCR 4.2	The system shall be fully integrated with other systems as required to enable the following: Control and monitoring of access points integrated with the Spectator Electronic Access Control System;	TDO,SSOC
PCR 4.3	The system shall be fully integrated with other systems as required to enable the following: Control and monitoring of the Active Hostile Vehicle Mitigation (HVM) barrier system;	TDO,SSOC
PCR 4.4	The system shall be fully integrated with other systems as required to enable the following: Monitoring intercom call location;	TDO,SSOC
PCR 4.5	The system shall be fully integrated with other systems as required to enable the following: Monitoring of fire alarm activation;	TDO,SSOC
PCR 4.6	The system shall be fully integrated with other systems as required to enable the following: Control and monitoring of lift car and hall call;	TDO,SSOC
PCR 4.7	The system shall be fully integrated with other systems as required to enable the following: ACS and IDS displayed on control room video-wall display system; and	TDO,SSOC
PCR 4.8	The system shall be fully integrated with other systems as required to enable the following: Live video and full control, functionality and configuration of any selected CCTV camera.	TDO,SSOC
PCR 4.9	The system shall be fully integrated with other systems as required to enable the following: Monitor and control of all door contact sets, motion detection sensor and duress/panic alert buttons.	TDO,SSOC
PCR 4.10	Seamless integration with the PSIM for Graphic Maps, Alarm, event, reports and incident management. SDK and API will be shared for the integration.	
PCR 4.11	Shall have the ability to Integrate with any Command & control systems (NCC / HUB etc.)	

1.3.3.2 Reliability Requirements

Backup, Restore & Archiving

No	Description	Stakeholder
RR 1.1	The ACS shall allow backup of important data such as the server database for avoiding loss of data in the event of hardware or software failure (such as a hard disk crash) occurs, files are accidentally deleted or in the event of a natural disaster, such as a flood or fire.	TDO,SSOC
RR 1.2	Backup strategies shall be predefined based on the types of situations that can occur: • Media failure—if one or more disk drives fails, there is a potential for a complete loss of data unless the system was properly backed up; • User error—if a user makes invalid modifications to data, for example, modifying detection settings, an effective way to undo these changes is to restore the data from backup; Permanent loss of a server, if a server becomes permanently unusable, for example, due to natural disaster.	TDO,SSOC
RR 1.3	Backups are a CPU and disk intensive operation on a large system, and therefore back-ups shall routinely be assigned to quiet times on the network.	TDO,SSOC
RR 1.4	No data shall be lost if the ACS database is corrupted or destroyed.	TDO,SSOC
RR 1.5	SQL server databases with a daily backup job configured automatically when ACS is installed shall be copied from the ACS server to another location in case of hard disk failure	TDO,SSOC
RR 1.6	The System Integrity Service shall automatically run the following tasks: • Daily backup - This shall perform a complete backup of the database at 01:45 every day except Sunday. Daily backups are automatically deleted after seven (7) days; • Weekly backup - This shall perform a complete backup of the database at 01:45 every Sunday. Weekly backups are automatically deleted after twenty-eight (28) days; • Monthly backup - This shall perform a complete backup of the database at 03:45 on the last day of every month. Monthly backups are automatically deleted after ninety (90) days.	TDO,SSOC

1.3.3.3 Security & Privacy Requirements

User Access

No	Description	Stakeholder
SPR 1.1	The following is a sample list of stakeholders or users who will use the system. Additional users shall be added and roles can be defined. The system shall protect the privacy of people whose actions are recorded by the system. Each access point shall be set to allow change of status once authorization is received from a supervisor/manger, thus preventing operators from reviewing or overriding predefined access control rights without good reason or permission.	TDO,SSOC

No	Description	Stakeholder
SPR 1.2.1	The user/role is identified in tabular form below: - Operator: Capacity to view and control the system. The user shall possess system operation knowledge.	TDO,SSOC
SPR 1.2.2	The user/role is identified in tabular form below: - Supervisor: Capacity to view, control, analyse and report on the system. The user shall possess system operation knowledge.	TDO,SSOC
SPR 1.2.3	The user/role is identified in tabular form below: - Maintenance Technician: Capacity to view, control and maintain the system. The user shall possess system operation & basic configuration knowledge	TDO,SSOC
SPR 1.2.4	The user/role is identified in tabular form below: - Engineer: Capacity to configuration of the system. The user shall possess detailed system configuration knowledge.	TDO,SSOC
SPR 1.2.5	The user/role is identified in tabular form below: - Manager: Super User, ability to have full configuration and administration of the system. The user shall possess detailed system configuration and administration knowledge.	TDO,SSOC

1.3.3.4 User, System & Support Documentation Requirements

Training & Handover

No	Description	Stakeholder
DOC 1.1	Training tailored to the Khalifa International Stadium implementation, shall be provided to the user groups listed in 1.3.3.3 in addition to security stakeholders and Client representatives.	TDO,SSOC
DOC 1.2	Training shall be user group / role-specific and include the following delivered in English and Arabic: - Manuals; - Presentations; and - Live system demonstrations.	TDO,SSOC
DOC 1.3	The entire training documentation such as Operator Manuals, Administrators Manuals, Configuration Manuals, presentation material, system design document and User account shall be tailored to the Khalifa International Stadium implementation and shall be submitted for review and approval prior to the training programme.	TDO, SSOC

1.3.3.5 Testing Requirements

Testing & Commissioning

No	Description	Stakeholder
TR 1.1	Stress/Load Testing: Stress/Load testing to be performed to ensure that the system operates effectively without loss of performance in realistic, high network traffic conditions.	TDO, SSOC
TR 1.2	User Acceptance Testing: User Acceptance Testing of system to demonstrate full functionality and performance in accordance with specified requirements and agreed use-cases.	TDO, SSOC
TR 1.3	Integrated User Acceptance Testing: This will demonstrate full functionality of integration between the system and other systems and services.	TDO, SSOC

1.3.3.6 Service / Warranty / Maintenance:

No	Description	Stakeholder
WS 1.1	Service Level Agreement (SLA) shall be documented signed along with contract for the Support and Maintenance.	TDO, SSOC
SW 1.2	Terms & Condition for warranty and duration period shall be done in contract period.	TDO, SSOC

2. References

Following is the list of references.

- Security Design Guide Q22M-APW-CMN-PMC-STR-0790 Rev 1;
- ICT Standards and Specifications Criteria for Sports Venues SC-I60-CAF-TEC-STD-00001;
- Q22M-PMC-1378 - Emiri Decree 9 2011 - Video Surveillance.