Annex B: Technical Schedules A/B for CCTV system

TECHNICAL SCHEDULES A & B FOR

SPECIFICATION FOR CCTV SURVEILLANCE WITH INTRUDER DETECTION STANDARD IN ACCORDANCE WITH ESKOM STANDARD 240-91190304

Schedule A: Purchaser's specifications

Schedule B: Guarantees, compliance and technical particulars of equipment offered

The clauses and numbering in this table are not necessarily the verbatim clauses as per 240-91190304. Therefore it is OBLIGATORY on the TENDERER to review the applicable clauses in 240-91190304 in order to provide an informed response.

When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:

Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations

Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.

Do Not Comply - Conformation of Non-Compliance to ALL requirements in the applicable section

Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section if required.

Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section.

	Description	Schedule A	Schedule B (Supplier's statements of compliance)	References/ Statement (supporting evidence) & Deviations
3.6	Installation			
3.6(a)	To ensure quality workmanship and sound installation practice, it is imperative that the contractor adheres to the specifications and standards supplied by Eskom.	Comply		
3.6(b)	Only contractors with experience in CCTV and alarm system installations shall do installations. To this end the tenderer shall provide a CV of relevant experience and references.	Comply and provide supporting evidence		

3.6l	All installers shall adhere to the OHS Act (Occupational Health and Safety Act) of 1970 when installing the system. Contractors and sub-contractors shall meet the requirements specified by Eskom Health and Safety specifications	comply		X
3.6(d)	All equipment shall have a mechanical earth connected to the site earth according to Eskom standards.	comply		X
3.6(e)	All equipment shall be designed and specified for a minimum realisable operational life 10 years under the prevailing environmental conditions unless otherwise agreed to by Eskom during the tender evaluation stage.	comply and provide the design MTBF (Mean Time Between Failures)		
3.6(f)	Consideration must be given for the minimum working and electrical clearances of overhead equipment – see Eskom Specification 34-3–4 - Substations, Section 2: Generic Substation Design [–] - section 4.5.1.2	comply		X
3.6(g)	All equipment shall be labelled in accordance with the design diagrams, with durable, weather resistant labels.	comply		X
3.6(h)	Cable and wiring marking shall be in accordance with Eskom standard 240-64636794, Standard for Wiring and Cable Marking in Substations.	comply		X
3.6(i)	All cables and wires shall be marked with a unique identification, at all terminations, in accordance with the cabling and wiring diagrams supplied.	comply		X
3.6(j)	All of the splices and connections shall be mechanically secure and shall provide electrical contact without stress on connections and terminals.	comply		X
3.6(k)	Any hole which insulated conductors pass through shall be provided with a smooth, rounded bushing, or shall have smooth, rounded surfaces upon which the insulated conductors may bear.	comply		X
3.6(l)	Wireways shall be smooth and free from sharp edges, burrs, fins, or moving parts that may damage wiring.	comply		X
3.6(m)	All internal wiring connections shall be made with a solder lug or pressure terminal connector	comply		X

3.6(n)	A terminal lug shall be arranged such that in any position it cannot contact the metal enclosure, non-energized accessible metal parts or other electrical circuits. Alternatively the shank of the lug shall be provided with insulation equivalent to that of the conductor.	comply		
3.6(o)	Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.	comply		
3.6(p)	The CCTV installation shall be signed off as accepted by Eskom's appointed Project Engineer for the security system installation.	comply		
3.7	System Level			
3.7.1	System Overview			
3.7.1.1	On site			
3.7.1.1(g)(i)	On site different subsystems will communicate with various controllers (DVR, Alarm panel, PA controller etc.) using a combination of hardwired contacts and communication busses (RS232, Ethernet, proprietary protocols etc.). These controllers will communicate with each other as necessary to create a system which can meet the functional requirements set forth in this document.	comply		
3.7.1.1(g)(ii)	At manned sites there may also be a security monitoring station on site from which CCTV and alarms can be viewed.	comply		
3.7.1.1(g)(iii)	The security equipment cabinet shall also serve as the point of power distribution for the security equipment which may need a variety of combination of AC and DC power at various voltage levels.	comply		
3.7.1.2	Eskom Local OT Security Server			
3.7.1.2(i)	All sites with CCTV systems will communicate with a Local OU Security Server. This server shall be owned and hosted by Eskom. VMS server software will be housed here as well as other server related equipment such as alarm base stations.	comply		
3.7.1.2(ii)	If necessary due to budget/resource availability, the server can be hosted at a third party	comply		
3.7.1.3	Local Security Control Centre			

3.7.1.3(i)	The Local Security Control Centre shall be responsible for responding to alarms from sites and managing incidents on site using the CCTV data from site. Ideally the Local Security Control Centre should be an Eskom manned centre, but budget and resource restraints may necessitate that the control centre be provided by a third party. Network security between any 3rd parties and the Eskom Network shall be designed and controlled by Eskom.	comply		
3.7.1.3(ii)	The Security Control Centre shall use approved VMS client software to connect to the Eskom OT Security Server, thereby receiving all alarm signals from the various sites (black screen monitoring). The Local Control Centre shall also be able to receive video on demand from the sites via the OT Security Server.	comply		
3.7.1.3(iii)	The connection between the Local OT Security Server and the Local Security Control Centre shall be a dedicated link (e.g. a Diginet line / microwave link). There may also be a backup links directly between the Local Security Control Centre and sites if this is deemed necessary.	comply		
3.7.1.4	National Security Control Centre			
3.7.1.4(i)	Eskom intends to establish an Eskom National Security Control Centre from which selected security incidents can be managed and monitored. A communication link would be established from the local OU security servers to the National Control Centre server via the Eskom corporate LAN. Selected signals or events would then be directed to the National Security Control Centre. It shall be possible to escalate events from the Local Security Control Centre to the National Security Control Centre.	comply		
3.7.1.5	Engineering and Operational Access			
3.7.1.5(i)	Eskom engineers shall be able to connect to the Local OT Security Server remotely from the Eskom Engineering (OT) LAN to perform maintenance and administrative tasks on the system.	comply		

3.7.1.5(ii)	Members of Eskom Group Security shall be able to connect to the OT security server remotely from the Eskom corporate network in order to perform operational tasks (check up-time of systems, confirm sites are being armed etc.) and investigations (view footage and alarm logs etc.).	comply		
3.7.1.5(iii)	This remote access shall be restricted to those who have explicitly been granted access rights.	comply		
3.7.3	Warrantee and Certification			
3.7.3(a)	All equipment installed shall be subject to the OEM warrantee	comply & provide OEM agreement letter		
3.7.3(b)	Contractor shall provide proof that technicians have been trained and certified to install and configure the CCTV equipment specified.	comply & provide training certificates for technicians		
3.7.3(c)	There shall be an agreement from the OEM that the OEM supports the tender offering and will continue to support the product if the tenderer defaults.	comply & provide OEM support agreement		
3.7.4	General Physical Requirements			
3.7.4.1	Environmental conditions			
3.7.4.1(a)	Ambient air temperature: -25 °C to +55 °C (installed indoors); or -25 °C to +70 °C (installed outdoors, within enclosures).	comply and provide reference		
3.7.4.1(b)	Altitude: < 2 500 m	comply and provide reference		
3.7.4.1(c)	Pollution: Location in urban areas with industrial activities and without special precautions to minimize the presence of sand or dust (conditions as per classes 3C2 and 3S2 in IEC 60721-3-3[12]).	comply and provide reference		
3.7.4.1(d)	Relative humidity (24h average): 98%	comply and provide reference		
3.7.4.1(e)	All outside equipment Including fasteners and supports should be corrosion resistant and appropriate for the environment on site	comply and provide reference		
3.7.4.1(f)	After fabrication, metal surfaces including doors and removable covers shall be prepared and finished with corrosion protection.	comply and provide reference		

3.7.4.1(g)	Paint work damaged during transport and delivery shall be made good as per manufacturer repair specification at no cost to Eskom. If site re-painting is necessary, the equipment and labels shall be carefully masked and any overpaint which occurs in spite of the masking must be removed. If the damage is not repairable, Eskom reserves the right to return the equipment.	comply		
3.7.4.1(h)	All nuts, bolts and washers use for the construction to be stainless steel. Screws can be cadmium plated.	comply		
3.7.4.1(i)	Further environmental protection may be needed e.g. Equipment installed at a coal power station or in a mining area will need added dust protection.	comply		
3.7.4.1(j)	Convection cooled (fan-less) equipment are strongly preferred. If fans are used, they shall be speed controlled and the electronics shall be isolated and conformal coated to protect against dust ingress.	comply and provide reference		
3.7.5	General Electrical Requirements			
3.7.5(a)	The expected life of equipment under conditions specified (section 3.7.4.1 above) shall be a minimum of 10 years.	comply and provide the design MTBF (Mean Time Between Failures)		
3.7.5(b)	All power cable shall be appropriately sized to ensure voltage drops along cable runs remain within the operating specifications of the equipment being powered.	comply		
3.7.5 (c)	All equipment shall be effectively protected against overvoltage due to lighting strikes or switching surges by strategically placed surge arrestors	comply		
3.7.5(d)	Descriptive cable markings shall be used as agreed to with Eskom. These shall be reflected on the drawings.	comply		
3.7.5(e)	Cable selection and routing shall always be done in such a way that operation of equipment is not affected by electrical interference. This may be achieved by separating power and communications cables, shielding of cables, or a combination of the two.	comply		
3.7.5(f)	Equipment shall not be affected by electrostatic discharges that are applied directly to the equipment or to metal objects in the proximity of the equipment: All electronic equipment shall be a class 2 device as specified in IEEE 1613-2009, 8 Electrostatic discharge tests[24]	comply and provide reference		

3.7.6	Cable routes in control plant / equipment rooms:			
3.7.6(a)	Auxiliary power cables shall be laid in the control room power rack, away from communication cables. No conduit is needed on the rack.	comply		
3.7.6(b)	Communications cables should use the control plant room communications rack. No conduit is needed on the rack.	comply		
3.7.6(c)	Where cable racks are not available, cables may be routed along the wall or in PVC sleeves in the cable trench, at Eskom's discretion.	comply		
3.7.6(d)	Where security cables are routed along the walls, they shall be in metal or plastic conduit.	comply		
3.7.6(e)	Auxiliary power and communication cables shall be in separate conduit.	comply		
3.7.6(f)	In substations, security cables shall not be routed in the ceiling.	comply		
3.7.6(g)	If fibre optic leads are used they should be protected usi36unctiogue tubing when entering and exiting cable trays or panels.	comply		
3.7.6(h)	Regional or site specific requirements may supersede the above cable route requirements.	comply		
3.7.7	Outdoor Cables and Trenching in Substations			
3.7.7(a)	Security cable should share control cable or lighting trenches where possible, where this is not possible, security cable trenches shall be dug.	comply		
3.7.7(b)	The security cables shall enter the control plant room through the same path as control cables.	comply		
3.7.7(c)	Security cable trenches shall be 0,5 m deep	comply		
3.7.7(d)	All cables shall be armoured or laid in appropriately sized plastic conduit (e.g. HDPE, Kabelflex, whether in cable trenches or dedicated security trenches. The appropriate bends and connectors must be used for the conduit, according to manufacturer's instructions.	comply		
3.7.7(e)	Security systems communication cables and auxiliary power cables shall not be laid in the same conduit unless using fibre communication or DC power.	comply		

3.7.7(f)	Drilled holes in junction boxes shall be kept to a minimum and shall be appropriately sealed to prevent water ingress.	comply		
3.7.7(g)	Care shall be taken when working with fibre optic cable so as to ensure the fibre is not damaged during installation or maintenance.	comply		
3.7.7(h)	The stone layer shall be removed far enough from the cable trench excavation as illustrated in 6. The trench soil shall not be placed on top of any yard stone.	comply		
3.7.7(i)	After the cables have been laid, the trenches must be backfilled with the original soil in layers not exceeding 300mm and properly compacted. Once the backfill is completed, the stone shall be replaced appropriately.	comply		
3.7.8	Security Cabinet			
3.7.8(i)	The security cabinet/panel shall contain all the control equipment of the intruder detection and the surveillance system (digital video recorder (DVR), communication equipment, public address (PA) etc.). The cabinet shall be housed within a suitable access controlled equipment room.	comply		
3.7.8(a)	The cabinet shall comply to Eskom Standard 240-6072564“, "Specification for Standard (19 inch) Equipment Cabin”ts". The Cabinet shall be a freestanding standard equipment cabinet (600 x 600). For servers, a freestanding server cabinet shall be provided.	comply		
3.7.8(b)	Cabinet shall be designed so as to limit dust ingress which could affect effective operation of equipment.	comply		
3.7.8(c)	All points of cable entry shall be through glands so as to secure the cables.	comply		
3.7.8(d)	Access to the inside of the cabinet shall be restricted and controlled by means a physical lock to which only authorized security personnel and Eskom employees from the Risk Department shall have access. Cabinet shall be alarmed for tempering and remain armed when main alarm system is disarmed. This is subject to regional requirements.	comply		
3.7.8(e)	Cabinet design shall take into consideration airflow and heat distribution. Equipment shall be laid out such that units that generate the most heat are at the top.	comply		

3.7.8(f)	There shall be a dedicated Aux power supply distribution module with a suitably sized incomer isolator and suitably sized load MCBs per piece of equipment	comply		
3.7.8(g)	The incomer supply DB MCB for this module must be correctly sized to protect the incomer cable in order to prevent nuisance trips.	comply		
3.7.8(h)	Cables shall be neatly routed in trunking.	comply		
3.7.8(i)	Cable ties or similar shall be used for cable management.	comply		
3.7.8(j)	Where possible equipment in the security cabinet shall be 19 inch rack	comply		
3.7.8(k)	Equipment or connection accessed regularly shall be accessible from the front of the panel or shall be wired to a terminal rack accessible from the front.	comply		
3.7.8(l)	Equipment shall be suitably earthed to the cabinet, and the cabinet shall be earthed to the substation earth.	comply		
3.7.8(m)	Eskom shall approve the layout design before the cabinet is populated.	comply		
3.7.9	Backup Power Supply			
3.7.9(i)	The responsible Eskom DC design engineer shall be consulted on a per site basis to determine which power supply system will be used and to allocate connection MCB's on the main Distribution Board.	comply		
3.7.9(ii)	The supply shall include a battery backed up UPS for all security system devices.	comply		
3.7.9(iii)	The standing time for backup power is 12 hours at sites within 200kms of a responsible Eskom DC section, 18 hours at sites more than 200kms from a responsible Eskom DC section.	comply for 12 hours		
3.7.9.1	Option A: 220V DC			
3.7.9.1(a)	The security system shall be powered by 220V supplied from the site's DC supply. In the event of a power failure the system will be supplied by the substation's battery and / or generator backup.	comply		
3.7.9.1(b)	The security system shall be supplied by an appropriately sized supply cable and MCB from the site's DC panel.	comply		
3.7.9.1c)	The MCB used on the AC/DC panel shall be clearly labelled 'Security'.	comply		

3.7.9.1(d)	Power will be distributed through the panel so as to isolate the supply of the subsystems by means of appropriately sized MCBs. At a minimum the following will be on separate supply circuits:			
	i. Intruder detection system	comply		
	ii. Perimeter Cameras	comply		
	iii. DVR, Indoor cameras and PTZ	comply		
	iv. Perimeter detection system (if separate from perimeter cameras)	comply		
	v. Other security related equipment such as motorized gates or electric fences.	comply		
3.7.9.2	Option B: 220V AC			
3.7.9.2(a)	Alternatively the security system shall be powered by 220V AC supplied from the site's AC supply with an appropriately sized Uninterruptable Power Supply. With this option, the requirements above shall still be complied with.	comply		
3.7.9(f)	CCTV system batteries in addition to UPS batteries are not recommended. If CCTV system batteries are unavoidable then individual subsystems that have their own battery backup, these shall not be fed by the UPS. This is to prevent the UPS from charging these batteries in the event of a power failure (See figures 10 and 11). Any CCTV system batteries used shall provide backup for the time specified in section e) above.	comply		
3.7.9(g)	The system shall have a power failure intruder detection indication that shall be sent through to the security control room should the AC supply be interrupted.	comply		
3.7.9(h)	The system may have an additional power failure alarm indication that shall be sent through to Eskom network control via SCADA should the AC supply be interrupted.	comply		
3.7.10	Communication			
3.7.10(a)	A connection from the site to the Eskom local OT security server shall provide the means of communication to the control centre for, alarms and live viewing.	comply		
3.7.10(b)	The connection shall also be used for remotely configuring equipment and downloading of recorded footage	comply		

3.7.10(c)	The communication link between the site and the security control room shall be by means of a dedicated and secure communication medium between the sites and the security control room.	comply		
3.7.10(d)	The systems must be capable of communication over Eskoms telecommunications network	comply		
3.7.10(d)(i)	When specifying a new site Eskom Telecoms will be consulted to determine the feasibility of using (or establishing) an Eskom Telecoms link to the site.			
3.7.10(d)(ii)	Eskom Telecoms will be consulted before going out on tender and communications available shall be stated at tender phase.			
3.7.10(d)(iii)	The priority and risk at the site shall be taken into account when deciding whether or not to increase bandwidth available for security			
3.7.10(e)	Though the Eskom telecommunication network is preferred, 3rd party communications infrastructure may be used if necessary.			
3.7.10(f)	The communication medium will be fibre (2Mbps bandwidth) where possible and satellite or microwave where fibre is not installed.	comply		
3.7.10(g)	As a last resort, if a higher bandwidth connection is not possible, GPRS may be used for communications provided equipment is specified and configured to be operated over the lower bandwidth.			
3.7.10(i)	The connection from the security equipment to the Eskom Telecoms network shall be Ethernet	comply		
3.7.10(j)	Eskom to provide all IP addresses to be used for on-site LAN.			
3.7.12	Time Synchronisation			
3.7.12(a)	In order accurately analyse recordings of incidents, and for providing reliable evidence, recorded footage needs to be time stamped with an accurate date and time stamp.	comply		
3.7.12(b)	The preferred method of time synchronization is using GPS. If a site has a GPS time signal, it should be used for the security system.	comply		

3.7.12(c)	At a single site, all cameras shall be time synced to within 1s of each other. This time syncing may be provided by the DVR or other timing device.	comply		
3.7.12(d)	Different sites shall be synchronised so that the difference between the times at different sites is less than 10s. This synchronisation may happen via an NTP clock or the central video management system (VMS).	comply		
3.7.12(e)	The central NTP clock or VMS system shall get its time from a GPS signal.	comply		
3.8	Intruder Detection System			
3.8.1	Indoor Detection			
3.8.1(a)	There shall be intruder detection in all buildings and rooms which the risk assessment indicates should be protected. At substations this will include all rooms of the relay house and switch rooms.	comply		
3.8.1I(b)	The sensors shall be placed so as to detect intrusion through any door or window leading into the building or by which access can be gained into the secured area.	comply		
3.8.1(c.)	Intruder detection may be in the form of movement detection (e.g. passive infrared sensors (PIRs), video analytics); door and window detection (e.g. Reed switches), or some combination of sensors.	comply		
3.8.1(d)	Intruder detection shall be located as to detect unauthorised entry through any door or window in the building.	comply		
3.8.1(e.)	Battery rooms holding lead acid batteries are a zone 2 hazardous location with specific rules governing work in the room. For this reason battery rooms shall not have CCTV or alarm equipment installed inside, but rather a door contact installed on the outside of all doors and windows to detect unauthorised entry.	comply		
3.8.2	Alarm System Operation			
3.8.2(a)	The alarm system shall meet the requirements of Eskom specification 240-867389–8 - Standard for Security Alarm Systems for Protection of Eskom Installations and its Subsidiaries [3]. In addition, the alarm system shall support the following when integrated with the CCTV:	comply		

3.8.2(b)	When an alarm is generated by the alarm system, the CCTV system shall detect the alarm and know what zone was triggered in ordered to trigger the relevant cameras for that zone.	comply		
3.8.2(c)	The alarm system shall receive trigger signals from CCTV video analytics in addition to triggers from the site's traditional security sensors.	comply		
3.8.2(d)	For redundancy alarm signals shall be sent to the Local OT security server through the CCTV system (to the VMS) and well as through the alarm system (to the alarm base station).	comply		
3.8.2(e)	The intruder detection system shall be able to control relay contacts which can be connected to the gate motor for opening and closing the gate.	comply		
3.8.2(f)	Should the intruder detection system be triggered at night, the site's LED floodlights shall be activated for a period of 15 minutes. Night can be determined by a means of day/night sensor or a clock timer. See section 3.8.3 below for more details.	comply		
3.8.2(g)	When the alarm is deactivated, a signal shall be sent through to the security control room identifying the employee who disarmed the site.	comply		
3.8.2(h)	Alarm system activation / deactivation shall be confirmed by means of audio sound over the speaker system as well as indicator LED(s) visible from inside the relay house and from the outside the gate of the site.	comply		
3.8.2(i)	Activation/deactivation of the intruder detection system shall activate/deactivate perimeter detection and internal building protection whether the detection is on the cameras or alarm sensors.	comply		
3.8.2(j)	Each activation / deactivation of the alarm system shall be date and time stamped and recorded by the alarm system.	comply		
3.8.2(k)	The system shall use remote controls to activate and deactivate the system as specified by 240-86738968 or per the technology already being used in the region.	comply		
3.9	Yard			
3.9.1	Yard overview			

3.9.1(a)	The main outdoor area to be covered by the CCTV and intruder detection system shall be along the perimeter of the facility within the boundary fence.	comply		
3.9.1(b)	There shall be a thorough analysis of the site's layout before installing any cameras and perimeter detection to ensure that the entire site perimeter has been covered. Once installed, the entire system will be tested to ensure that this intended coverage has been achieved (See sections 3.16.–0 - Indoor Intruder Detection Tests and 3.16.12 -Camera Functional Test).	comply and provide proposed camera location schematics/diagrams		
3.9.1(c)	The intention is for the perimeter detection system to detect when an intruder crosses the boundary of the site and the camera system to be used to verify that a person has crossed the boundary. The perimeter detection can be provided by video analytics, either as part of the camera / DVR, or as an add-on feature to the camera system. See Section 3.9.3.	comply		
3.9.1(d)	One or more PTZ cameras shall be installed so as to view the majority of the yard. The intention of the PTZ system is to automatically track intruders, providing information to the security monitoring centre which can be used to deter the intruder and guide armed response. At smaller, lower risk sites, the PTZ may be omitted to save costs. At other sites it may prove more feasible to use strategically placed fixed cameras instead of the PTz.	comply		
3.9.1(e.)	A fixed camera shall be positioned so as to have a clear view of the main entrance gate. The intention of the gate camera is to recognise people and vehicles entering the site.	comply		
3.9.1(f)	To prevent damage to the camera and ensure good picture quality, cameras shall not be placed in a direction such that they will be exposed to intense beams of light from the floodlights or direct sunlight.	comply		
3.9.1(g)	Visible notification shall be placed at entrances and on the outside of the perimeter fence of the premises to notify persons entering the premises, that they may be subjected to CCTV surveillance. At substations the date of placement of such notices shall be recorded in the substation logbook.	comply		
3.9.2	Perimeter Camera System Layout			

3.9.2 (a)	The installation of fixed cameras shall be done primarily to cover the inside perimeter of the site yard.	comply		X
3.9.2 (b)	The purpose of the perimeter cameras is detection (See section 3.9.1 for a discussion of camera purpose). Perimeter cameras shall provide control room operators a method to confirm when an alarm is generated that an intruder has breached / approached the perimeter.	comply		X
3.9.2 (c)	At selected sites it may be appropriate for the cameras field of view to cover the outside perimeter of the fence, supporting detection before the perimeter is breached. This will depend on detection method used and the likelihood of false alarms from movement just outside the perimeter.	comply		X
3.9.2 (d)	There shall be a thorough analysis of the site's layout before installing any cameras and perimeter detection to ensure that the entire site perimeter has been covered. This must include mapping each camera's field of view and range of view on the site layout drawings to ensure that the perimeter is 100% covered.	comply and provide proposed camera location schematics/diagrams		
3.9.2 (e)	The view of the camera shall be free of any hindering obstacles such as walls, trees or buildings.	comply		X
3.9.2 (f)	The installation of cameras shall be done so as not to hinder existing vehicle accessibility paths to the installed power plant.	comply		X
3.9.2 (g)	The recommended arrangement of cameras within a generic substation yard is illustrated in Figure 12. Achieving coverage of the yard fence need not always be by means of a camera installed parallel to the yard fence. This is especially the case where the layout of the yard is not square. The requirement is only to have visuals of all enclosing fences of the yard, be it a parallel visual along the span of fence or at an angle facing.	comply		X
3.9.2 (h)	Where it is possible to obtain visuals at an angle of the fence, it shall be ensured that there is no obstacle between the camera and the face of the fence being monitored.	comply		X
3.9.2 (i)	Perimeter cameras shall be arranged so that the dead spot of each camera is covered by the field of view of another camera as shown in Figure 12.	comply		X

3.9.2 (j)	Should there be obstacles or poor visuals, additional cameras shall be installed to cover the span of fence.	comply		
3.9.3	Perimeter Detection System			
3.9.3 (a)	Alarms shall be generated by a perimeter detection system.	comply		
3.9.3(b)	The use of microwave beam detection is strongly discouraged due to the prevalence of nuisance alarms.	comply		
3.9.3 (c)	The perimeter detection can be provided by 'video analytics', either built into, or as an addition to, thermal perimeter cameras. Other detection methods (or combination of detection methods) may be used if they are able to meet the functional requirements specified here.	comply and provide supporting documentation		
3.9.3(d)	If Video analytics is used it should be 'advanced video analytics', able to analyse the footage, not simply video motion detection which only looks for changes in the picture. See Annex A for the distinction between the two.	comply		
3.9.3(e)	Edge' video analytics is preferred over server/DVR based video analytics. Edge video analytics happens on board the camera or on a device connected to each camera. Each camera therefore has a dedicated processor analysing its footage. Server or DVR based analytics uses one processor to analyse the feeds from a number of cameras, increasing the chance of poor performance. See Annex A for more information.	comply		
3.9.3(f)	The perimeter detection system shall create an 'invisible wall' which encapsulates the entire perimeter of the yard, so that there are no areas where an intruder may enter the site undetected.	comply		
3.9.3(g)	There shall be no 'dead spots' in the invisible wall. Where a method of detection has an inherent dead spot, the dead spot of each device shall be covered by another device (e.g. Cameras with overlapping fields of view).	comply		

3.9.3(h)	The perimeter detection method should be divided into zones matching the areas covered by the perimeter cameras. This shall enable the operators at the security control room to determine which area has been disturbed and which visual to use from the camera covering that section of fence where the incident occurred. Zone names must be the same on site as in the video management system at the security monitoring centre. These zones and zone names shall be reflected on the site layout provided with the system documentation.	comply and provide supporting documentation		
3.9.3(i)	The perimeter detection system must generate an alarm when a human enters the monitored zone. It must be able to detect a person who is walking upright, walking hunched over, crawling or running.	comply		
3.9.3(j)	The system must not be triggered by changes in light, movement of trees, small vibrations of the camera pole, animals including birds, vehicles driving past the protected siyte, weather conditions such as rain and snow.	comply		
3.9.3(k)	The sensitivity of the perimeter detection system must be adjustable in order to configure the system to meet the conditions at specific sites.	comply		
3.9.3(l)	The system must be able to operate in all lighting and weather conditions.	comply		
3.9.3(m)	Nuisance alarms shall be limited to 7 nuisance alarms, per site, per 7 day period.	comply		
3.9.3.1	Poles			
3.9.3.1(a)	Where lighting poles, buildings, or other suitable structures exist on the site in appropriate positions, these may be used to mount the cameras. If no existing structure is available, the cameras shall be mounted on poles.	comply		
3.9.3.1(b)	Poles shall be steel reinforced 4.5m or 5.7m spun concrete poles according to Eskom drawings: D-DT-0010 or D-DT0011. Poles may be purchased on the Eskom ENC (Eskom National Contract) if one is in place at the time.	comply		
3.9.3.1 (c)	Poles to be installed as per manufacturer instructions so as to minimize vibration due to wind.	comply		

3.9.3.1(d)	To prevent theft of cameras, the poles shall not be placed directly next to the fence, and anti-climbing devices shall be considered.	comply		
3.9.3.1(e)	The pole shall be earthed via 50 x 3 mm earth tails, the earth tails shall be buried and welded to the base of the fence so as not to be easily visible. The join shall be painted the same colour as the fence to avoid theft of the copper earthing.	comply		
3.9.3.1(f)	The earthing shall conform to the latest revision of the general earthing standards of copper joints as per D-DT-5240, sheets 2 and 6 (Annex C and Annex D)	comply and provide supporting evidence		
3.9.3.1(g)	Holes required for the fixing of the sensors and cameras may be drilled on-site and shall be appropriately sealed to prevent water ingress. Drilling can be minimised by using equipment that clamp securely onto the poles.	comply		
3.9.3.1(h)	Prior to the installation of the support foundation, the stone layer shall be removed sufficiently far enough from where the foundation is to be cast.	comply		
3.9.3.1(i)	On completion of the installation, all excess soil shall be removed from the yard and the stone shall be replaced to cover the area surrounding the foundation.	comply		
3.9.3.1(j)	All cabling be routed through the foundation of the cement pole. Drilled holes shall be kept to a minimum and shall be appropriately sealed to prevent water ingress.	comply		
3.10.	CCTV Surveillance System			
3.10(i)	The subcomponents of the surveillance system primarily consist of fixed perimeter cameras, gate cameras, PTZ cameras, indoor cameras and the security and site lighting. It is recommended that when any design is done, that it be taken into consideration that should the equipment need upgrading, that the existing infrastructure shall be able to incorporate new technologies.	comply		
3.10.1	Camera Purpose			
3.10.1(i)	In order to test whether a camera is fit for purpose, it is essential that the purpose of this camera be defined.			

3.10.1.1	Each camera shall have a single, clearly defined purpose. The purpose should consist of a category (detection, observation, recognition or identification), an area to be covered and a range of distances from the camera.	comply and provide supporting documentation		
3.10.1.2	Lighting conditions in which the camera should operate should also be stated.	comply and provide supporting documentation		
3.10.2	General Camera Requirements			
3.10.2.1	General			
3.10.2.1(a)	Cameras should be IP cameras, exceptions should be obtained for installation of analogue cameras	comply		
3.10.2.1(b)	Before installation begins the camera layout, including expected fields of view and dead spots, shall be documented and signed off by an Eskom Engineer.	comply		
3.10.2.2	Cables			
3.10.2.2(a)	Choice of cables shall be based on camera manufacturer recommendations.	comply		
3.10.2.2(b)	Either fibre or electrical signals may be used for camera communication. Cost should be considered when choosing between Cat 5 and fibre communication cables. In high EMF environments CAT6 or fibre should be considered.	comply		
3.10.2.2(c)	Where electrical cables are used they should be unshielded twisted pair (UTP) cable, such as CAT5. UTP cabling is cost efficient, has high noise immunity, lower loss per length than coax and allows for high quality long range transmission.	comply		
3.10.2.2(d)	For analogue cameras a UTP balun connector may be implemented for the cabling between the camera and the DVR. Cat5 is recommended over coaxial cable as it is thin and flexible cable making it easy to string between walls.	comply		
3.10.2.2(e)	Cable selection and routing shall always be done in such a way that operation of cameras is not affected by interference. This may be achieved by separating AC power cables from communication cables, shielding cables, or a combination of the two.	comply		
3.10.2.3	Installation			

3.10.2.3 (a)	The installation of the camera and brackets shall be as indicated in the manufacturer's guidelines.	comply and provide supporting documentation		
3.10.2.3(b)	Brackets used to secure the camera shall be robust and shall minimize vibration.	comply		
3.10.2.3(c)	Brackets shall be capable of being "lock tight" to reduce the possibility of accidentally moving.	comply		
3.10.2.3(d)	All brackets shall be "cable managed" so that cable entering the housing is enclosed within the bracket from the support to the housing, allowing no cable to be exposed.	comply		
3.10.2.3(e)	The cables shall be marked with at least the camera name and number.	comply		
3.10.2.3(f)	Dome and PTZ cameras shall be mounted with appropriate brackets which prevent the pole from being in the camera's field of view.	comply		
3.10.2.4	Manufacturer Specifications			
3.10.2.4(a)	Automatic Gain Control (AGC) shall be at least 30dB	comply		
3.10.2.4(b)	Back light compensation must be implemented.	comply		
3.10.2.4(c)	The camera's specified coverage distance shall be 10% further than is required by the site security design.	comply		
3.10.2.4(d)	Minimum Frames Frequency shall be 8 fps	comply		
3.10.2.4(e)	The lens shall be chosen to suit the application and the functional requirements of the site.	comply		
3.10.2.4(f)	If cameras are IP Cameras, they shall be ONVIF compliant.	comply and specify which open industry protocols are supported		
3.10.2.4(g)	Image Format shall be 1/3 inch or larger	comply		
3.10.2.4(h)	All cameras settings (except focal length and focus) shall be remotely configurable, either via the DVR, or directly using Ethernet.	comply		
3.10.2.4(i)	The camera shall provide a minimum horizontal resolution of 600 TV lines or 800 pixels.	comply		
3.10.2.4(j)	The signal to noise ratio shall be ≥ 52db.	comply		
3.10.2.4(k)	Camera shall implement wide dynamic range and white balance control functionality to compensate for bright areas.	comply		

3.10.2.4(l)	Camera shall have Wide Dynamic Range	comply		
3.10.3	General Requirements for Outdoor Cameras			
3.10.3(i)	Outdoor cameras shall meet all specifications listed in section 3.10.2 – General Camera Requirements	comply		
3.10.3.1	General			
3.10.3.1 (a)	As far as possible, outdoor cameras shall be positioned “North to South” in order to avoid sunlight on the lens. In some cases this is not possible; therefore all cameras shall have wide dynamic range (WDR) functionality.	comply		
3.10.3.2	Cables			
3.10.3.2(a)	The power cable shall be steel wire armoured cable.	comply		
3.10.3.3	Installation			
3.10.3.3 (a)	The camera shall be well protected from the elements and vandalism by mounting it within an appropriate housing.	comply		
3.10.3.3 (b)	The camera housing shall have an IP rating of at least 65.	comply and provide supporting documentation		
3.10.3.3 (c)	The camera housing shall have a sun visor and be steel constructed.	comply		
3.10.3.3 (d)	The camera housing shall be weather-proof, environmental, corrosion and vandalism resistant as well as UV resistant.	comply		
3.10.3.3 (e.)	Harsh environments such as coal power plants may require a harsh environment housing. Similarly cameras at coastal sites will need added corrosion protection.	comply		
3.10.3.3 (f)	If necessary, a junction box with a minimum rating of IP 65 may be installed on the camera support pole. The junction box shall be used to protect any connections and additional equipment necessary for the camera operation. Equipment housed in the junction box should be kept to a minimum; as much equipment as possible shall be housed in the equipment room / relay house.	comply		
3.10.3.3 (g)	If used, the junction box shall be mounted on the cement pole support, below the camera.	comply		

3.10.3.3 (h)	If used, the junction box shall be lockable (lock and key, not a panel key) and alarmed.	comply		
3.10.3.3 (i)	All openings of the housing and junction box, used as well as unused, shall be properly sealed to prevent any water or insects from entering the housing.	comply		
3.10.3.4	Manufacturer Specifications			
3.10.3.4(a)	outdoor cameras shall meet all requirements under 3.10.2.4 above	comply		
3.10.3.4 (b)	Camera sensor shall be protected from sun damage. Mechanical Shutters are susceptible to failure and will not be accepted.	comply		
3.10.4	Fixed Thermal perimeter cameras			
3.10.4.1	Introduction			
3.10.4.1(a)	The purpose of perimeter cameras is to provide confirmation of an intruder when an alarm is generated by the perimeter intruder detection system.	comply		
3.10.4.1(b)	Since the images from good thermal cameras are not affected by weather conditions (fog, rain, snow), or glare, it is preferred that the perimeter cameras be thermal. It is also preferred that these thermal cameras provide perimeter detection using 'video analytics', either built into, or as an addition to, the perimeter cameras.	comply		
3.10.4.2	Specifications			
3.10.4.2(i)	Thermal cameras shall meet all specifications listed in section 3.10–2 - General Camera Requirements,	comply		
3.10.4.2(ii)	Thermal cameras shall meet all specifications listed in section 3.10–3 - General Requirements for Outdoor Cameras.	comply		
3.10.4.2(iii)	If video analytics on the cameras is used as a method of intruder detection, the video analytics shall meet all specifications listed in 3.9–3 - Perimeter Detection System.	comply		
3.10.4.2(a)	Thermal perimeter cameras shall be installed along the perimeter of the site yard as described in section 3.9.2 above.	comply		
3.10.4.3	Manufacturer Specifications			
3.10.4.3(i)	Thermal cameras shall meet all requirements under section 3.10.2.4 above	comply		

3.10.4.3(ii)	Thermal cameras shall meet all requirements under section 3.10.3.4 above	comply		
3.10.4.3(iii)	Detector type shall be Uncooled micro bolometer	comply		
3.10.4.3(iv)	Thermal cameras must have Automatic Gain Control	comply		
3.10.4.3(v)	Resolution shall be at least 320 x 240	comply		
3.10.5	Fixed perimeter cameras – non thermal			
3.10.5(i)	Fixed cameras shall meet all specifications listed in section 3.7.4 – General Camera Requirements,	comply		
3.10.5(ii)	Fixed cameras shall meet all specifications listed in section 3.10–3 - General Requirements for Outdoor Cameras.	comply		
3.10.5(iii)	Fixed cameras shall be installed along the perimeter of the site yard as described in section 3.9.2 above.	comply		
3.10.5(iv)	If non thermal perimeter cameras are to be used, the design must explicitly address how the effects of weather will be mitigated.	comply and provide supporting documentation		
3.10.5.1	Manufacturer Specifications			
3.10.5.1(i)	fixed perimeter outdoor cameras shall meet all requirements under 3.10.2.4 above	comply and list any deviations		
3.10.5.1(ii)	fixed perimeter outdoor cameras shall meet all requirements under 3.10.3.4 above	comply and list any deviations		
3.10.5.1(iii)	Infrared shall Use 850 or 940nm wavelength. Distance covered must match application.	comply and provide supporting documentation		
3.10.5.1(iv)	The minimum sensitivity shall be 0.0002 lux for colour images and 0.00002 lux for monochrome images.	comply and provide supporting documentation		
3.10.6	PTZ camera			
3.10.6.1	Introduction			
3.10.6.1(i)	The purpose of the PTZ cameras is to track intruders in order to help response teams pinpoint the location of intruders. Intruder tracking can be automatic or manual.	comply		
3.10.6.2	Installation			
3.10.6.2(a)	One or more PTZ cameras may be installed within the yard depending on the risk and the layout of the site.	comply		

3.10.6.2(b)	The PTZ camera shall be positioned in the yard in such a way as to cover the majority of the critical points. Positioning shall be site dependent and shall be informed by the site PSD,	comply		
3.10.6.2(c)	In the case where there are no perimeter cameras, the perimeters and the critical points to be covered by the PTz.	comply		
3.10.6.2(d)	Where there are perimeter cameras the critical points to be covered by the PTZ are: cable trenches, Building Entrance,Gate entrances, Minisubs, RMUs or Metering Kiosks, Outdoor storage areas	comply		
3.10.6.2 (e.)	The PTZ camera unit shall be installed in one of the following manners:			
3.10.6.2 (e.)(i)	On a 7.2m or 9.1m Eskom approved cement pole (See D-DT-0011& D-DT0012 for guidance). The installation shall be done according to the latest revision of D-DT-0332 (LV and MV Foundation Pole Arrangement).	comply		
3.10.6.2 (e.)(ii)	A steel pole attached to a building. SANS 1431 grade 300WA or 4360 grade 43A steel shall be used.	comply and provide supporting documentation		
3.10.6.2 (e.)(iii)	A bracket attached to an already installed Eskom lighting mast.	comply		
3.10.6.3	Specification			
3.10.6.3(i)	PTZ cameras shall meet all specifications listed in section 3.10–2 - General Camera Requirements,	comply and list any deviations		
3.10.6.3(ii)	PTZ cameras shall meet all specifications listed in section 3.10–3 - General Requirements for Outdoor Cameras.	comply and list any deviations		
3.10.6.3(a)	The PTZ's zooming capabilities shall be powerful enough to meet the purpose of the PTZ	comply		
3.10.6.3(b)	The PTZ camera shall be remotely controllable by an operator to pan, tilt, zoom, focus, mobilize the iris, switch the camera on/off and place the camera in a pre-set position.	comply		
3.10.6.3(c)	The PTZ camera shall be controlled by a hardwired cable.	comply		
3.10.6.3(d)	If there are no perimeter cameras then the PTZ shall be able to see the perimeter by means of thermal imaging or a built in infrared spotlight.	comply		

3.10.6.3(e)	The PTZ shall have preset positions. When a preset position is chosen by the controller, the PTZ shall immediately go to that position.	comply		
3.10.6.3(f)	Preset positions shall include zoom level.	comply		
3.10.6.3(g)	It shall be possible to label the preset positions with a descriptive name.	comply		
3.10.6.3(h)	The PTZ shall be capable of having at least 10 pre-sets.	comply		
3.10.6.3(i)	Preset positions at each site shall include all gates, doors, various points on the perimeter boundary and high risk assets (trenches, transformers, rolls of cable).	comply		
3.10.6.4	Operation			
3.10.6.4(a)	It is preferable that the PTZ have built in analytics and be set to 'patrol' the yard during normal operation.	comply		
3.10.6.4(b)	If the PTZ does not have analytics then during normal operation it should be set to a useful 'home' position (e.g. gate).	comply		
3.10.6.4(c)	When an alarm triggers the PTZ shall zoom into the area where the alarm happened. If a person is detected, the PTZ shall follow the motion of that person.	comply		
3.10.6.4(d)	The control signals from an operator shall take preference over the patrol and tracking functions.	comply		
3.10.6.4(e)	Preset positions at each site shall include all critical points on the site.	comply		
3.10.6.5	Manufacturer Specifications			
3.10.6.5(i)	PTZ camera shall meet all requirements of section 3.10.2.4 above	comply and list any deviations		
3.10.6.5(ii)	The minimum Pan speed at which the PTZ camera can pan the full 360° shall be 6° per second	comply		
3.10.6.5(iii)	The Pan Range angle through which the PTZ can tilt shall be minimum 90º (-10º +80º)	comply		
3.10.6.5(iv)	Minimum Optical Zoom which the camera can zoom without reducing resolution shall be 3.2mm – 138.5mm (43x) (Site dependent)	comply		
3.10.6.5(v)	Minimum digital zoom that camera can zoom while decreasing the resolution shall be 16x	comply		

3.10.6.5(vi)	The minimum light sensitivity shall be 0.0007 lux for colour images and 0.000007 lux for monochrome images.	comply and provide supporting documentation		
3.10.7	Indoor Cameras			
3.10.7(i)	At substations, indoor cameras shall be installed in control plant rooms and switch rooms.	comply		
3.10.7(ii)	Indoor cameras shall meet all specifications listed in section 3.10.2 – General Camera Requirements	comply		
3.10.7.1	General			
3.10.7.1(a)	The camera field of view shall include the entrance to the room/building as the point of interest. Where there is more than one entrance, more indoor cameras may be necessary, as determined by the risk assessment.	comply		
3.10.7.1(b)	Indoor cameras may be dome, fixed or bullet cameras	comply		
3.10.7.1(c)	Indoor cameras shall have infrared lighting.	comply		
3.10.7.1(d)	The purpose of the camera shall be observation and / or identification in the case of forced entry depending on the site requirements.	comply		
3.10.7.1(e)	Backlight compensation with wide dynamic is particularly necessary for cameras looking at entrances.	comply		
3.10.7.2	Placement and Installation			
3.10.7.2(a)	Indoor cameras may be ceiling or wall mounted depending on the site.	comply		
3.10.7.2(b)	The camera shall be housed in a vandal proof housing with an IP rating of at least 51.	comply		
3.10.7.2 (c)	The camera field of view shall be adjustable via an adjustable bracket or built in manual pan-tilt mechanism.	comply		
3.10.7.3	Manufacturer Specifications			
3.10.7.3(i)	Indoor cameras shall meet all requirements listed in 3.10.2.4	comply and list any deviations		
3.10.7.3(ii)	Camera shall have day/night function to compensate for poor lighting conditions	comply		
3.10.7.3(iii)	Electronic shutters shall be used to compensates for moderate light changes in indoor applications without the use of auto iris lenses.	comply		
3.10.7.3(iv)	Camera shall have infrared.	comply		

3.10.7.3(v)	The minimum illumination shall be 0.0002 lux for colour images and 0 lux for monochrome images.	comply and provide supporting documentation		
3.10.8	Digital Video Recorder / Network Video Recorder			
3.10.8(i)	A Digital video recorder (DVR) or Network Video Recorder (NVR) shall be used to record relevant video footage as well as to allow access to live streaming footage from the security control room.	comply		
3.10.8(ii)	The DVR shall be integrated with the alarms from both the perimeter detection system and the indoor intruder detection system and shall connect to the Video Management System.	comply		
3.10.8(iii)	The DVR shall meet all specifications listed in section 3.7.4 – General Physical Requirements, and section 3.7–5 - General Electrical Requirements	comply and list any deviations		
3.10.8.1	DVR Functionality			
3.10.8.1(a)	In the event of an alarm being triggered (from camera or intrusion detection system) when the system is armed the system shall cater for the followi56unctionalityity:			
3.10.8.1(a)(i)	Record footage from relevant cameras.	comply		
3.10.8.1(a)(ii)	The footage recorded shall be for 5s second before the event triggered, the time of the actual event (however long motion is detected by the camera) and at least a 15 second post event time period. This recording shall be at the full resolution of the camera.	comply		
3.10.8.1(a)(iii)	Send a signal to the Security Control Room, including the zone that was triggered.	comply		
3.10.8.1(a)(iv)	Send short video clip / series of still pictures from the camera covering the zone where the alarm triggered to the security control room.	comply		
3.10.8.1(a)(v)	Allow for the security control room to remotely access the site in order to stream live footage from the system.	comply		
3.10.8.1(a)(vi)	Allow for the security control room to operate any PTZ cameras installed on site, including using pre-set positions.	comply		
3.10.8.1(a)(vii)	Allow for the controller to speak over the PA system or play a pre-recorded message on site.	comply		

3.10.8.1(b)	In the event of movement being detected when the system is not armed, the system shall: Record footage from relevant cameras for 5s second before the event, the time of the actual event (For however long motion is detected by the camera) and at least a 15 second post event time period. This recording shall be at the full resolution of the camera.	comply		
3.10.8.2	Compatibility:			
3.10.8.2(a)	The DVR shall be able to integrate with a wide range of cameras from different manufacturers.	comply		
3.10.8.2(b)	The DVR shall be ONVIF compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.	comply and specify which open industry protocols are supported		
3.10.8.2(c)	The DVR shall allow for simultaneous use of different model cameras with different resolutions.	comply		
3.10.8.3	Recording and streaming			
3.10.8.3(a)	It shall be possible to configure the DVR to record on any motion event or only when an alarm event is generated.	comply		
3.10.8.3(b)	Simultaneous recording on site and streaming to the security control room shall be possible.	comply		
3.10.8.3(c)	It shall be possible to stream video at a lower resolution and frame rate than the footage is recorded on site.	comply		
3.10.8.3(d)	Recording: Shall be such that identification can be achieved on cameras with identification as the purpose.	comply		
3.10.8.3(e)	All footage shall be time and date stamped	comply		
3.10.8.3(f)	It shall be possible to search events and recorded footage based on a combination of date, time, event and motion in a specific part of the camera's field of view	comply		
3.10.8.3(g)	The recording media shall be a removable, hot swappable and lockable.	comply		
3.10.8.3(h)	All footage shall be kept for a minimum of 30 days. To achieve this, the hard drive size should initially be calculated to be large enough to store 30 hours of continuous recording from all cameras.	comply		
3.10.8.3(i)	It shall be possible to 'flag' important footage so that it will not be overwritten.	comply		

3.10.8.3(j)	When the hard drive is full, the DVR shall continue to record by overwriting the oldest recordings first. Flagged footage shall not be overwritten.	comply		
3.10.8.4	Frame Rate			
3.10.8.4(a)	The frame rate shall be adjustable	comply		
3.10.8.4(b)	A frame rate of at least 25fps shall be achievable by the DVR	comply		
3.10.8.4(c)	Recommended frame rate for streaming video: 2-5 fps	comply		
3.10.8.4(d)	Recommended frame rate for recordings: 6fps or larger	comply		
3.10.8.5	Video Compression			
3.10.8.5(a)	Compression standards such as H. 264, MPEG4 or equivalent may be used for streamed video	comply and provide supporting documentation		
3.10.8.5(b)	A compression standards such as MJPEG or equivalent may be used for streamed video	comply and provide supporting documentation		
3.10.8.5(c)	Video compression shall be used appropriately such that the specified purpose of each camera (detection/observation/recognition/identification) can be achieved for recordings and streaming of footage	comply		
3.10.8.6	Time Sync			
3.10.8.6(a)	The DVR shall enable the syncing of time between sites, and between cameras as specified in section 3.7.12	comply		
3.10.8.7	Remote Connections			
3.10.8.7(a)	It shall be possible to remotely view live or recorded video over the network (with appropriate access rights).	comply		
3.10.8.7(b)	It shall be possible to configure all DVR settings over the network (with appropriate access rights).	comply		
3.10.8.7(c)	It shall be possible to download recordings on site or offsite.	comply		
3.10.8.8	Video Monitor			
3.10.8.8(a)	It shall be possible to plug a Video Monitor into the DVR (site specific)	comply		
3.10.8.9	Security			
3.10.8.9(a)	The DVR shall be password protected.	comply		

3.10.8.9(b)	The DVR shall cater for a minimum of 10 individual users with assigned access rights	comply		
3.10.8.9 (c)	There shall be a minimum of 2 access levels, one with limited access right, the other with full administrative rights	comply		
3.10.8.10	Hardware and I/O connections			
3.10.8.10(a)	The DVR shall have input contacts for connecting to alarm signals from the alarm system	comply		
3.10.8.10(b)	It is recommended that DVR have an 'error' output which will output a signal to the alarm system if there is an error with the DVr.	comply		
3.10.8.10(c)	DVR shall have an on off switch and status LED	comply		
3.10.8.11	System Logging:			
3.10.8.11(a)	The DVR shall keep a time stamped electronic log of the following:			
3.10.8.11(a)(i)	User who has logged in to make changes.	comply		
3.10.8.11(a)(ii)	Changes made	comply		
3.10.8.11(a)(iii)	System Errors	comply		
3.10.8.11(a)(iv)	Interruption of Camera feeds	comply		
3.11	Video Management System (VMS)			
3.11.1	Introduction			
3.11.2	Location and Architecture			
3.11.2(i)	In regions where an Eskom security control room for remote sites is not available, the security control shall be manned and hosted by a contractor. It is however imperative that Eskom still remains in control of the VMS infrastructure and is not locked into using one service provider indefinitely. For this reason a distributed architecture shall be used for the security network allowing for the VMS system to be used from multiple secure sites.	comply and provide supporting documentation		
3.11.2(ii)	The network infrastructure shall adhere to the principles laid out in the following Eskom Documents			
3.11.2(ii)(a)	240-554109–7 - Cyber Security Standard for Operational Technology	comply and provide supporting documentation		

3.11.2(ii)(b)	240-556835–2 - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities	comply		
3.11.2.1	Hosting Server at a Third Party – Exceptional Case			
3.11.2.1	There may be cases where, due to budget, infrastructure or resource restraints, it is not feasible for the server to be hosted by Eskom. In such cases the VMS server may be hosted by a third party.	comply		
3.11.2.1 (a)	There shall be an agreement with the third party as to who owns the Servers, VMS software license, Configuration data, Recordings and Logs when the contract expires	comply		
3.11.2.1 (b)	There shall be a strategy for moving monitoring of sites to a different third party, or Eskom premises when the contract expires.	comply		
3.11.3	Network and Connections			
3.11.3(a)	The VMS shall connect to CCTV cameras and DVRs via the Eskom OT network, a third party network, or a combination of the two.	comply		
3.11.3(b)	The VMS shall be capable of a 'Client-Server' configuration. The server shall be housed at an Eskom site and the security control room shall connect to the server using client software, over a secure, dedicated link.	comply		
3.11.3(c)	Authorised Eskom employees using the client software shall be able to connect to the server via the Eskom Corporate Network.	comply		
3.11.3(d)	The VMS system shall be able to connect to a minimum of 500 sites and 4000 cameras. Not all installations will need this many connections, but it shall be possible to upgrade the system to accommodate these numbers.	comply and provide supporting documentation		
3.11.3(e)	The VMS design shall cater for failover and allow for a redundant architecture.	comply		
3.11.3(f)	The system shall allow for at least 5 simultaneous client connections.	comply		
3.11.3(g)	The frame rate and resolution of camera connections shall be reduced in order to provide smooth footage over the communication medium.	comply		
3.11.4	Features			

3.11.4(a)	The VMS shall be able to connect to a wide range of CCTV NVRs and DVRs.	comply and provide supporting documentation		
3.11.4(b)	Where there are already CCTV components installed, the VMS shall be compatible with the existing install base of CCTV equipment.	comply		
3.11.4(c)	The VMS system shall be ONVIF Compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.	comply and specify which open industry protocols are supported		
3.11.4(d)	The VMS shall be able to connect to cameras with a wide range of different resolutions (from CIF (352x240) to 5 Megapixel). Typically the higher resolutions will only be used when monitoring is on site.	comply		
3.11.4(e)	All security control room activities as described in section 3.12 Security Control Room, shall be possible using the VMS system.	comply		
3.11.4(f)	The VMS system shall allow for Access Control integration.	comply		
3.11.4(g)	The VMS shall be linked to an NTP/SNTP timeserver to synchronise the time on the VMS system.	comply		
3.11.4(h)	The VMS shall be able to operate as a time server to synchronise the times of downstream systems at remote sites.	comply		
3.11.4(i)	The VMS shall allow an administrator to make customizable reports on events, system status etc.	comply		
3.11.4(j)	The VMS shall allow the security control room operators to view whether a site is armed or disarmed.	comply		
3.11.4(k)	It shall be possible to draw up a list of all sites which are disarmed.	comply		
3.11.5	Network Security			
3.11.5(a)	The system shall comply with 240-55410927: Cyber Security Standard for Operational Technology which serves to guide the implementation of Cyber Security principles in the OT environment	comply and provide supporting documentation		
3.11.5(b)	All connections to the Eskom OT networks shall be firewalled as per 240-79669677: Demilitarised Zone (DMZ) Designs For Operational Technology	comply		

3.11.5(c)	All connections to the Eskom corporate network shall be firewalled and approved by Eskom Group It.	comply		
3.11.5(d)	Remote Access to the Eskom network shall adhere to 32-273: Information Security – IT/OT and Third Party Remote Access Standard.	comply		
3.11.5(e)	The Engineering design shall follow both IT and OT governance processes as per 240-55863502: Definition of OT and OT/IT Collaboration Accountabilities.	comply		
3.11.5(f)	The VMS shall allow for individual, password protected user rights.	comply		
3.11.5(g)	There shall be a minimum of the following 2 access levels:			
3.11.5(g) (i)	Level 1 shall provide viewing of footage only, with no ability to delete footage or view and change network settings.	comply		
3.11.5(g)(ii)	Level 2 shall provide full administrative rights.	comply		
3.11.5(h)	The system shall keep a time and date stamped log of all logon events	comply		
3.11.5(i)	The system shall keep a log of all administrative changes made on the system, including who made the change.	comply		
3.11.6	Video Recording and Streaming			
3.11.6(a)	The primary purpose of the VMS shall be to view live footage. Due to network constraints the primary place for saved recordings shall be on site. However, for investigation and training purposes, it shall be possible for the VMS to record footage which has been streamed to the security control room and to export that footage.	comply		
3.11.6(b)	The VMS shall support simultaneous recording and streaming of footage.	comply		
3.11.6©	The VMS shall support streaming at a wide range of resolutions, depending on the network bandwidth and the camera being connected to.	comply		
3.11.6(d)	The VMS shall enable different client workstations to stream from different cameras simultaneously.	comply		
3.11.6(e)	The VMS shall enable a continuous streaming ‘video wall’. This shall be customizable, allowing for resizable viewing panes.	comply		

3.11.6(f)	The VMS shall support recording and playback of files using H.264, MPEG and MJPEG video compression	comply and provide supporting documentation		
3.11.6(g)	The VMS shall be able to trigger recordings based on: Schedule, Manual trigger, alarm, event	comply		
3.11.6(h)	The VMS shall be able to stream and record using various frame rates (8fps - 25fps). Typically the higher frame rates will only be used for live footage when monitoring is on site.	comply		
3.11.6(i)	The VMS shall be able to use a wide range of different communication links to different sites. This will range from poor 3G connections, to high latency satellite, to fibres. It shall be possible to cater for different frame rates and resolutions per site depending on the bandwidth and cost of the communication medium.	comply		
3.11.6(j)	All recordings shall be electronically watermarked and show time and date.	comply		
3.11.6(k)	It shall be possible to search events and recorded footage based on a combination of date, time, event and motion in a specific part of the camera's field of view	comply		
3.11.6(l)	Playback in slow motion and at high speed shall be possible.	comply		
3.11.6(m)	The player shall allow for multichannel playback, which allows users to play recorded video from several cameras simultaneously. This is useful if tracking suspects moving on a site.	comply		
3.11.6(n)	The system shall be able to perform mass export of archived footage.	comply		
3.11.6(o)	It shall be possible to 'cut' footage to export only the portion of footage that is of interest	comply		
3.11.6(p)	As a guideline, the system shall cater for at least 7 days of continuous recordings from each of the security control room monitors, streaming from 5 of the highest frame rate and resolution cameras installed.	comply		
3.11.6(q)	It shall be possible to 'flag' important footage so that it will not be overwritten.	comply		
3.11.6(r)	When the hard drive is full, the oldest recordings shall be overwritten first. Flagged footage shall not be overwritten.	comply		
3.11.7	Event Management			
3.11.7	The VMS shall support the following event management functions			

3.11.7(a)	Support 'black screen monitoring': In normal state, no video is shown. When an alarm triggers at a site the controller sees a series of still images or a short video clip of the zone where the alarm was triggered. The controller can then choose to stream video from the site.	comply		
3.11.7(b)	Support an event queue to allow the management and acknowledgment of multiple alarm events.	comply		
3.11.7(c)	It shall be possible to look at a new event without having acknowledged a previous event.	comply		
3.11.7(d)	Support PTZ control including PTZ pre-set positions.	comply		
3.11.7(e)	Allow the transmission of voice from the controller to the PA system on site.	comply		
3.11.7(f)	Allow for the controller to control lights at the site.	comply		
3.11.7(g)	Allow controller to view the location of alarms and cameras on a site layout	comply		
3.11.7(h)	Allow controller to view the location and status of all sites on a map	comply		
3.11.7(i)	Enable comments from controller to be linked to an event.	comply		
3.11.7(j)	It shall be possible to 'escalate' incidents to another workstation running the client software e.g. another controller or an Eskom National Security Control Centre.	comply		
3.11.7(k)	Log events and actions for auditing purposes	comply		
3.11.7(l)	A highly recommended feature is the ability of the VMS system to track movement and highlight which area of the camera field of view has triggered an alarm (This could be software based or a feature of the cameras or video analytics on site).	comply		
3.11.8	Usability			
3.11.8	The VMS system shall have high usability (be 'user friendly'). Usability is a difficult thing to quantify but can be broadly defined as consisting of:			
3.11.8(a)	The system shall be easily learnable	comply		
3.11.8(b)	The system shall be highly efficient	comply		
3.11.8(c)	The system shall be easily memorable	comply		
3.11.8(d)	It shall be easy to recover from errors	comply		

3.11.8(e)	It shall be pleasant to use the design	comply		
3.11.8(f)	Before choosing a VMS system Eskom shall view a demonstration of the VMS product. The service provider shall be able to demonstrate all of the features specified above, this shall include administrative tasks as well as security control room tasks. The evaluator(s) shall use the system themselves as part of this demonstration rather than simply being shown the system in operation.	comply		
3.11.9	Hardware			
3.11.9(a)	Server shall meet Eskom IT requirements for servers including:			
3.11.9(a)(i)	An HP server may be used	comply		
3.11.9(a)(ii)	Server shall be 19” rack mountable	comply		
3.11.9(a)(iii)	The operating system shall be approved by Eskom IT	comply		
3.11.9(a)(iv)	Symantec antivirus shall be installed (can be provided by Eskom IT support)	comply		
3.11.9(a)(v)	Server shall connect to Eskom IT servers for antivirus and Windows security updates.	comply		
3.11.9(b)	Server shall meet with the VMS manufacturer’s hardware requirements.	comply		
3.11.9(c)	Server shall be housed in a secure, access controlled environment.	comply		
3.11.10	Training and Support			
3.11.10(a)	There shall be local support for the VMS product.	comply		
3.11.10(b)	There shall be product support in the closest City to the installation	comply		
3.11.10(c)	The tenderer shall provide Eskom with details of their support network as well as the service levels in terms of turnaround time to attend to technical problems.	Comply and to provide details of support network as well as the service levels in terms of turnaround time to attend to technical problems.		
3.11.10(d)	Operator and administrator training shall be provided	comply		
3.11.10(e)	Documentation on the hardware installation shall be provided	comply		
3.11.10(f)	Instruction manuals shall be provided	comply		
3.12	Security Control Room			

3.12.1	The CCTV surveillance shall be monitored by Eskom staff or an Eskom approved security company located within a secured central security control room.			
3.12.2	The security control room shall be equipped such that the security control room operators shall, for each site, be able to execute the following functions:			
3.12.2 (a)	Select each individual camera within the site to view footage from the respective camera.	comply		
3.12.2 (b)	Select a program to sequentially switch the cameras.	comply		
3.12.2 (c)	Operate the zoom, pan and tilt throughout the complete range of each PTZ camera installed.	comply		
3.15	Maintenance			
3.15.1	Introduction – Maintenance Contracts			
3.15.1(a)	All installations shall be accompanied by a 1 year maintenance contract.	comply		
3.15.1(b)	After this 1 year period one of the following must be in place:			
3.15.1(b)(i)	A maintenance contract with a supplier	comply		
3.15.1(b)(ii)	A maintenance plan for Eskom to do maintenance work.	comply		