Security Operations Centre Design Considerations Guide

GCPSG-003 (2021)

Prepared By:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
Departmental Security Branch
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication Issued: 2021-08-09

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Forward

The Security Operations Centre Design Considerations Guide is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

This is a Government of Canada publication to serve as a guide to assist in the design of a Security Operations Centre for departments, agencies and employees of the Government of Canada.

Suggestions for amendments and other information can be sent to the RCMP Lead Security Agency RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Effective Date

The effective date of the Security Operations Centre Design Considerations Guide is 2021-08-09.

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment

Note: Authority for modifications or variances is the RCMP LSA.

Contents

1. Contact Information

For more information, please contact:

Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #165
Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

2. Abbreviations and Acronyms

Abbreviation / Acronym	Meaning
ANSI	American National Standards Institute
BIMFA	Business and Institutional Furniture Manufacturer's Association
BMS	Building Management System
CAD	Computer Aided Design
CATV	Cable Television
CPU	Central Processing Unit
CSA	Canada Standards Association
EMS	Emergency Medical Services
ER	Equipment Room
ERS	Emergency Response Services
HVAC	Heating, Ventilation, Air Conditioning
IP	Internet Protocol
IPTV	Internet Protocol Television
ISO	International Standards Organization
KVM	Keyboard – Video – Mouse
OGD	Other Government Departments
PBX	Private Branch Exchange
PC	Personal Computer
POTS	Plain Old Telephone System
RCMP	Royal Canadian Mounted Police
RDS	Room Data Sheet
SOC	Security Operations Centre
SPC	Speech Privacy Class
TBD	To Be Determined
TIA/EIA	Telecommunication Industries Association /Electronic Industries Alliance
TV	Television
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VOIP	Voice – Over – Internet – Protocol

3. Introduction

3.1. Purpose

The purpose of the Security Operations Centre Design Considerations Guide is to provide a summary of options to be considered during the process of designing and building a Government of Canada (GC) Security Operations Centre.

3.2. Background

Security programs in place at many GC organizations include the creation and operation of a Security Operations Centre (SOC). A SOC provides operational and other security services to the department including the protection of people, property, assets and information. The SOC usually contains the facilities within which system operators can monitor, display and manage information (applications, video, and alarm systems) and then dispatch and respond to events. The design and development of a SOC should identify all areas to accommodate personnel, equipment and supplies associated with control, alarm and event monitoring activities. The design should also support the SOC requirements in relation to technical systems and equipment and operational use the space and its facilities.

3.3. Application

This guide has been developed assist users who design, re-design, or validate a new or existing SOC. It can be used to assist multi-disciplinary teams consisting of; property or facility, physical security, IT security, architects, engineers, and other service providers or designers.

3.4. Assumptions and Limitations

This guide attempts to summarize the many operational, architectural, and technical considerations that designers should consider in the development of a SOC. This guide is not an exhaustive or detailed design document rather it is a guide to assist project stakeholders to deliver a right-sized and functional SOC. The following assumptions and limitations are present in this Guide:

a. These guidelines are general regardless of the type of equipment selected;
b. Considerations are flexible and scalable to support all GC departments;
c. The space types described in the guide are, the SOC, and the SOC Control Suite. The SOC includes the SOC Control Suite and all supporting spaces. Supporting spaces are defined by the needs of the department and are out of scope for this guide. They may be managed through a Real Property functional programming process; and
d. The SOC designers may choose to use the standards and references provided in Section 8, to assist during the detailed design phase of the project.

3.5. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT) security, the requirement to assess the risk of any application and/or software connected to a network to operate and support equipment in Government of Canada controlled buildings is critical. Some examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC etc.

Before implementing any applications and/or software that will control and/or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the components the applications and/or software controls are maintained and that any risks highlighted will be mitigated. Starting the SA&A process early is highly recommended to ensure project delivery schedules are not affected. For more information on the SA&A process, please consult your departmental Security.

3.6. Project Planning and Phases

The project planning process can be described as a typical accommodations or technology adoption process. A departmental Facility Security Assessment and Authorization (FSA&A) and an IT Security Assessment and Authorization (SA&A) (if an SA&A is required) should be used when designing a SOC. Projects will have a number of phases with each phase depending on the outputs of the previous phase. Below shows a typical SOC Project Framework. Phases will vary depending on the complexity of the project, but should follow this typical approach:

- Project Charter;
- Project Statement of Intent;
- SOC Objectives;
- Functional and Technical Requirements;
- Concept of Operations;
- Concept design;
- Prototypes;
- Detailed Design including System Architecture;
- Technical Specifications and Statement of Work;
- Procurement;
- Implementation Plan;
- Installation;
- Programming and Configuration;
- Commissioning;
- Documentation; and
- Training.

4. Objective of a Security Operations Centre

4.1. Purpose

The purpose of a SOC is to provide a facility to support security personnel in the monitoring, surveillance, display, control, management and response to security-related events. A SOC typically provides 24 hour surveillance activities through video cameras, intrusion alarm sensors and related systems. The SOC also provides the ability to detect and respond to alarm conditions and dispatch staff to deal with the issue such as Contract Security teams, Commissionaires or Emergency Services personnel.

4.2. Functions

There are a number of critical functions carried out within the SOC and situational awareness is at the forefront of the operational purpose. Operators in the SOC:

a. Collect information related to the controlled and monitored environment;
b. Analyze the information to determine the impact or on a given situation; and
c. Respond to the situation appropriately.

4.3. Location

The locating of the SOC within a facility requires planning and operational consideration. Thought should be given to unique operational requirements such as mobility (alternate locations) and emergency procedures. Typically, the SOC should be out of sight but within audible range of the public. Operational and departmental requirements will dictate whether it should be an Operations or Security Zone (refer to RCMP LSA Guidance on the Application of Physical Security Zones) however access control should be strictly enforces in the SOC. During the functional programming stage of the project, its location, adjacencies, circulations and proximities can be defined.

5. Operational Considerations

5.1. Introduction

It is important to consider the operational requirements of the SOC before, during and after completion. Understanding of how the SOC functions is vital to the success of the project. In general, operational issues to consider include: operating hours (e.g., 24/7), occupancy loads, operator security clearances, policies and procedures, post orders, operator task rotations, skills and experience, backup/redundancy of equipment, client services options (if your SOC will service clients for any reason), and training requirements.

It is also vital that the SOC be planned, audited and analyzed to ensure a clear understanding of needs to be integrated in the new design. This planning work can be done in several ways:

a. Visiting or consulting with the existing SOC or other GC SOC's (if possible);
b. Reviewing existing policies and procedures, and current post orders;
c. Liaising operators and supervisors to obtain information pertinent to the SOC; and
d. Consulting with suppliers and consultants who can provide information about their own experience.

5.2. Scope of Operational Considerations

The Scope of Operational Considerations will be defined early in the design process. A useful framework for defining the scope is to identify all inputs and outputs to the SOC. While the specifics of the work environment will dictate the scope of operational considerations, following are sample inputs and outputs for a "typical" SOC:

Inputs:

- Radio, Telephone and Security Intercom Communications;
- Emails and Activity Logs;
- Security Video Camera Views;
- Security Alarms and Events;
- Technical Alarms and Events;
- Staffing Calls and Communications; and
- Building Access Control.

Outputs:

- Dispatched Calls to Security Operational Teams;
- EMS Calls – Fire, Police, Ambulance;
- Access Control Authorizations and/or Denials/De-Activations;
- Alarm Display;
- Overtime Requests;
- Foot Patrol Monitoring and Dispatch;
- Executive and Management Briefings, Oversight; and
- Wide Distribution Emergency Notifications.

5.3. Ergonomics

Room, video wall and workstation layouts should be designed to maximize the effectiveness and efficiency of room operations. The optimal ergonomic design of the room and the

individual work positions should be addressed. The design should protect the staff from musculoskeletal disorders and injuries and maximize operational efficiency for the tasks at hand, as well as the interactions between SOC operators. The ergonomic design should meet national/local health and safety regulations and adhere to ergonomic best practices for SOC design and operations as found in ISO and other guidelines and regulations. These documents are referenced in Section 7.

Specific SOC ergonomic design guidelines and considerations are as follows:

a. All desktop control equipment (keyboards, touch-screens, joysticks, radio equipment, telephones, video and audio controls, etc.) should be within acceptable arm reach and arranged for operational efficiency and ergonomic use (ie. sit-stand desks);
b. Controls should be logically arranged to maximize ease of use when used together (e.g., Computer Aided Dispatch control sand radio operations);
c. Colours, icons and other display elements should follow organizational or GC standards and be arranged logically (e.g., linear by process);
d. Displays should be arranged with spatial awareness in mind – logically organized to match the environment being monitored and the systems used for response;
e. All monitors should be designed and selected to maximize screen resolution, contrast and colour definition, refresh rates, size, array-configuration and viewing angles for each application being displayed; and
f. Situational Awareness should be supported by consistent mapping displayed in the SOC. This ensures all operators are responding to events within the same context.

5.4. Work Positions

The SOC Designer will need to develop work position profiles in order to define the operational requirements for each console. This will support the overall technical and functional design of the SOC. Each work position will have distinct roles and responsibilities, but regardless, designers should consider the following general behavioral capabilities when defining the work position:

a. Standard Operating Procedures, including drills and simulated event situations;
b. System and application operations;
c. Video System camera views and numbering systems, including naming conventions;
d. Site geography display and interaction (and availability);
e. Situational Awareness tools and displays;
f. Information sharing and process hand-offs during events or crises; and
g. Backup and contingency positions and processes as is situationally required.

The nature of the environment served by the SOC and the volume and frequency of events managed will guide the selection of work position types and quantities, including adjacencies and proximities. Table 2 shows sample work positions, along with their “typical” functions, tasks and activities. These are illustrative examples only, as each environment will differ, depending on the business and functional needs of the security teams at the organization.

Work Position	Tasks & Activities	Adjacencies	# Per Shift
Alarm Management	Perimeter Doors Duress Alarms Intrusion Alarms	Security Video Monitoring & Dispatch Video Wall	TBD
Security Video Monitoring	Interior and Exterior Video Tours of Facility or Site Monitoring of Perimeter Entrances Monitoring of Screening and Scanning Areas	Dispatch Video Wall	TBD
Call Receipt	Code Blue Stations Elevators Accessible Washrooms Telephones Radios	Alarm Management Dispatch	TBD
Supervisor	Monitor/Manage all Work Positions	View to All	TBD

Table 2 Work Position Planning

5.5. Shift Schedules

The operational plans and postures within the SOC are reflected in the Shift Plans and Schedules employed in the SOC. When the work positions are defined and the tasks and activities understood, the shift schedules can be planned. The development of the schedules will be based on the operational requirements defined for the SOC described in terms of:

a. Legislative requirements in the locale of the SOC;
b. Minimizing any negative health impacts to the general wellbeing of the operators;
c. The use of a variety of shift rotations and scheduled (ie. 8 or 12 hours shifts);
d. Expected workload, perceived stress, risk of errors and health risks;
e. Shift rotational design (rotate day-evening-night shifts in a predictable way);
f. An understanding of how shift schedules are tolerated by different team members;
g. Methods for providing choice on shift selection; and
h. Plans to detail how the overlap between shifts for shift-changeover briefings (update on happenings of the day and unresolved incidents) can maintain team situational awareness through the use of technology and tools.

5.6. Event/Threat Level Types

In advance of the technical design, the command and control postures for different situations need to be understood. Typically, the security operating environments are defined in terms of the business activities of the organization. The SOC team should define each of the different operating environments in terms of the SOC display, control and communications postures and capabilities of the technology and the team.

While the business needs of the organization will define these environments, a few samples demonstrate how the scenarios may be categorized:

a. Daytime Business Hours Standard Surveillance and Dispatch;
b. Nighttime and Silent Hours Perimeter Surveillance and Response; and
c. VIP Visit Route Coverage, Blue Force Tracking and Duress Monitoring.

The operating environment should be defined in terms of the tasks and activities assigned to each work position, the applications and video displayed on the video wall and the interactions and adjacencies of the work carried out.

5.7. Event and Activity Data

During the design phase of the SOC, it is important to understand the composition of event data and surveillance information received. Gather information from all existing operations; current activities, incident data, call volumes, alarm events, fixed and PTZ video surveillance camera feeds, application data, radio and telephony communications, fire and medical events and other activities within the current or planned SOC facility. The following table is an example, which could be used for gathering and analyzing event and activity data.

Description	Time	Time	Time	Time
Telephone Calls (IN))				
Intercom Calls (IN)				
Radio Calls (IN)				
Intrusion Alarms				
Number of Interior Fixed Cameras				
Number of Exterior Fixed Cameras				
Number of Exterior PTZ Cameras				
Dispatched Calls (OUT)				
Dispatch Radio Comms (OUT)				
Fire Alarms				
Fire Alarm Trouble Reports				
Medical Event Calls (IN)				
Other				
Other				

Table 3 – Event Data Capture

6. Architectural Considerations

6.1. Introduction

The first guiding principle is steering the development of the environment in which the SOC is located. A user-centered design is preferred which means the environment (and ultimately technology) is designed to support the activities of the control room personnel. Human factor-based design principles will address factors such as sight lines and memory and attention capacity. As these vary across individuals and tasks, the design needs to ensure a fit for the individual, the organization and the activities to be carried out in the room. Thoughts for any future expansion should be considered in the design phase.

6.2. Scope of Architectural Considerations

During the functional programming phase of the project, the architectural and space requirements will be defined in sufficient detail to move the project to concept design and to solicit input from the SOC user team members. The functional program will include planning options, project planning guidelines, flexibility and scalability strategies, shared support space requirements, adjacencies and proximities, infrastructure requirements (mechanical, electrical), occupancy estimates, furniture and equipment requirements, space details, connectivity details, special purpose space and security.

Each of the SOC spaces should be described in more detail in Room Data Sheets. As described, this guide focusses on the SOC Control Suite itself, and specific details for supporting spaces are out of scope for this guide. Designers should consider the following spaces for inclusion in the SOC:

a. Security Operations Centre Control Suite (SOC Control Suite);
b. Vestibule (between entry and SOC Control Suite);
c. Rest Area/Break Room;
d. Washroom/Shower/Changing Room(s);
e. Kitchenette;
f. Training Room;
g. Meeting Room;
h. Touch-Down Stations;
i. Security Equipment Room;
j. Equipment Storage Area;
k. Locker Room; and
l. Supervisor Office.

Room Data Sheets provide a more detailed description of the space requirements. Each space should have a separate Room Data Sheets and include:

a. Brief Functional Description;
b. Occupancy Load;
c. Required Area;
d. Preferred Location;
e. Primary Adjacencies;

f. Secondary Adjacencies;
g. Time of Use;
h. Architectural Requirements;
i. Floors, Partitions, Doors & Frames;
    - Door Hardware;
    - Windows & Glazing, Ceilings;
    - Speech Intelligibility, Noise Control, Speech Privacy;
j. Structural Requirements;
k. Mechanical Requirements;
    - Temperatures (unoccupied/occupied; summer/winter);
    - Humidity, Outdoor Air, Pressurization, Plumbing, Fire Protection;
    - Other operational requirements;
l. Electrical Requirements;
    - Normal Power, UPS/Emergency Power;
    - Lighting Types, Levels, Controls;
    - Fire Alarm;
m. Connectivity;
    - Voice, Data, Equipment, Multi-Media, Security, Other;
n. Security Requirements;
    - Levels, Requirements;
o. Furniture, Art, Equipment, Artifacts; and
p. Typical Layout (Drawing).

6.3. SOC Layout

There are many factors to consider in developing test and concept layouts of the SOC. Interactions, proximities, supervision, video wall views, sit-stand requirements, supporting infrastructure and facilities, oversight needs and other factors should be taken into account.

Typically, the size of the SOC Control Suite will be sufficient to provide space for the consoles, a video wall, other office equipment and the required circulation. The space should also support a defined number of personnel standing behind the console array, on the opposite end of the room from the video wall for crisis management and oversight purposes.

The following are topics for discussion during client-engaged space planning work:

a. The SOC Control Suite should be configured in such a way that each operator or supervisor, from his/her console may display, manage and monitor all systems, equipment and events from an integral display array on the console itself. Each operator should also have a full and complete view of the video wall from a sitting or a standing position;
b. Number of Console Work Positions required, including spare or overflow positions. Typical work positions are described later in this document;
c. Supervisor Console or facilities for oversight including number and location relative to the operator consoles and the supervisor office;
d. Console operators should be in close proximity to support the sharing of information and actioning of alarm response;

e. Discuss the work function and activities performed at each console and expected interaction with other operators to determine adjacency and proximity requirements. Interactions can include alarm verification between operators, passing verbal information to a dispatcher, incident identifier creation and communication, real-time decision making and communication, as well as real-time verbal updates;
f. Primary function definition (e.g., primarily video viewing at console and video wall vs. primarily dispatch functions);
g. Sightlines from console to video wall. Operators should have unobstructed sightlines from their operator consoles in either a standing or sitting position;
h. Define the room size, floor types and ceiling height after determining the operational considerations. With the front row of sit-stand consoles in the standing position, the ceiling height (and resultant video wall height) needs to provide each subsequent row of consoles with an unobstructed view of the video wall from the each Sit-Stand Console, in either sit or stand position. Position consoles around support columns to prevent obstructed views of the video wall for any one operator;
i. The SOC may also include supporting spaces such as rest areas, washrooms, kitchenette facilities, training rooms, multi-purpose meeting rooms, break-out and/or quiet rooms, touch-down stations, equipment storage areas (e.g., pylons, first aid kits, megaphones, security tape, etc.) lockers (or a locker room depending on its size) and supervisor areas. The types of supporting spaces (whether each are required), their locations and sizes will be determined during the design phase of the project;
j. The SOC should be equipped with raised access flooring for easy installation and access to cables, cable troughs, power and associated room/building services. The height of the raised floor will be dependent on the amount and type of infrastructure required and the available ceiling heights for video wall viewing;
k. Overheard speech can be a security concern and may be distracting. Acoustical attenuation, including low reflectivity surfaces and sound attenuating acoustical ceilings may be required. Normal ambient noise should be less than 55db. As well, the SOC should be considered a sensitive acoustical environment such that speech privacy is achieved from the control room (to outer, more public-spaces), sound protection may be needed between the equipment room and the control room and between any adjacent spaces and the control room. An SPC rating of 85 is typically recommended for the SOC control room;
l. Ensure to address any accessibility or mobility requirements so that GC, building code, organizational and other legislated standards are a part of the project;
m. Space for private conversations and/or planning should be designed into the area;
n. Variable light level controls for the SOC should be implemented to provide the operators with their desired ambient light conditions (e.g., full-spectrum light bulbs);
o. Wall space for standard white boards and/or large monitors will be required for daily information management such as shift change information, “today” bulletins, pass-along information and general information;
p. Bookshelves for Standard Operating Procedures, Policies and Procedures, Emergency Response Plans, Post Orders and Site Contact Lists. Much of this may be included in on-line Security Information Management Systems but hard copy documents will likely be needed.

6.4. Circulation

The movement of SOC personnel and other authorized occupants should be defined during the design process. The following design recommendations should be considered when a test layout is developed for the SOC:

a. Adequate provisions should be made for general circulation so that control operations are not interrupted;
b. Adequate circulation areas and routes should be developed for situations where shift changeover is protracted, and two shifts are in the space at the same time;
c. The layout of each room should allow for the orderly evacuation of the room;
d. Circulation routes should be designed to avoid cross-circulation;
e. For wheelchair users, allowances need to be made for the maximum width of the largest wheelchair and clearances for elbows to propel the chair. The recommended minimum clearances are 1200mm for length of wheelchair (including footrest and clearance) and 900mm for width of wheelchair and clearance; and
f. Wheelchair users will require additional space for turning, and these should be provided at appropriate locations in the SOC according to local building codes.

6.5. Room Lighting

Room and task lighting designs for the SOC Control Suite are of critical importance in the design of a safe and effective purpose-built workspace. The lighting design for the control suite should be flexible, optimize visual performance, improve legibility of information, enhance operator comfort and health and facilitate the reading and viewing of all displays.

The ISO 11064 standards provide detailed recommendations for lighting design in SOC Control Suite. The most critical of these are as follows:

a. Minimize any sources of glare on the operator work positions and the video wall;
b. Provide individual task lighting controls for operators;
c. Flexible lighting designs should be provided to account for future changes in the SOC Control Suite;
d. If natural light is present, it should be managed;
e. Specific light levels should be developed in collaboration with the SOC Control Suite Designer and the Electrical Engineering Designers;
f. Take into account ceiling and wall light reflections;
g. Designers should define lux levels for work surfaces, dimming maximums, paperwork illumination, glare indices, colour rendering indices, self-illuminated equipment characteristics, direct and indirect lighting sources and respective performance; and
h. Lighting should consider day vs night operations, the use of "red light" should be considered for night operations.

6.6. SOC Physical Security Requirements

The SOC should be designated as a Security Zone and be nested within an Operations Zone. This may vary depending on the nature of the organization, the purpose of the SOC, the nature and level of information reviewed and processed in the SOC and the nature of the business functions of the organization.

Nonetheless, following are guidelines for the physical security of the SOC. The organization should also define the priority for each physical security control measure by designating each as either "Mandatory" or "Nice-to-Have".

Item	Physical Security Requirement	Priority
1	Electronic Access Control into the SOC and SOC Control Suite (with Activity Log).	
2	Video Surveillance into SOC area and SOC Control Suite clear enough to identify all individuals entering through portals into each respective space. Note: this video coverage should not view the interior of the space.	
3	Duress Alarm buttons at each console work position which would alarm outside of the SOC at another designated location.	
4	Intrusion Alarm Devices on all portals into the SOC and SOC Control Suite.	
5	Located in a Security Zone; protected on all six sides from brute force entry attack; out of the view of the general public and visitors to the building.	
6	Adjacent Equipment Room providing computer and communications support for the SOC to be equipped with electronic access control, video surveillance of entries into the room.	
7	Video Intercom facilities outside the SOC Control Suite so that positive identification can be gained for all non-accredited individuals requesting entry into the Suite.	
8	Doors and Frames providing brute force attack protection.	
9	A vestibule outside the SOC should be equipped with an interlock using an electronic locking system such that the inner and outer doors cannot be open at the same time.	

Table 1 – Physical Security Requirements

7. Technical Considerations

7.1. Introduction

It is important to consider the technical requirements of the SOC before, during and after completion. Awareness of the department's current technical environment, equipment and system standards, networking and application hosting facilities and power availability are each vital to the success of the project.

In general, technical issues to consider include: electronic security systems, business applications, telephony and networking capabilities, communications methods and protocols, and other building and life-safety related systems. Interoperability or interconnectivity of these systems should also be considered.

7.2. Scope of Technical Considerations

The following technologies will, most likely, be considered in the design and implementation of a SOC, regardless of its size or complexity:

- Security Management Applications;
- Video Management System;
- Intrusion Alarm System;
- Access Control System;
- Telephony;
- Radio Communications;
- Security Intercom Systems;
- IT Infrastructure;
- Server and Workstation Computing Resources;
- Video Display Technologies;
- Video Wall Management Technologies;
- Integrated Consoles and Systems;
- Power distribution: UPS and Emergency Power;
- Fire Alarm Systems; and
- Other Systems, as required.

7.3. Audio Communications & Telecommunications

SOC operators communicate with a number of groups; each other, on-site security personnel, members of the organization at large, emergency response services and others, just to name a few. SOC designers will need to understand the organizational norms, interactions with others outside the organization and the tasks and activities of each operator before determining which types of communications services should be designed into the SOC. The following is a list of communications methods that may need to be considered:

a. Centrex or VOIP Telephone System – often each console operator has access to a telephone, which may be on the organization's network (ie. VOIP) or PBX (ie. Centrex or other handsets). Consideration should also be given to the provision of headsets (jacks can be integrated into the console) to enhance usability;
b. Security Intercom Master Stations – since most organizations have deployed audio

and/or video intercom substations across its premises (as well as outside the SOC), each operator often requires a means to communicate with individuals requesting support at a substation;

c. Analog Telephone Lines – operator clients will confirm whether a separate POTS (Plain Old Telephone System) two-wire line is required as backup into the SOC; and
d. Radio Communications – much design support will be required to ensure that there is sufficient coverage and on-console radio communications (and controls). In addition, many SOCs have agreements with local law enforcement to share radio channels, which should be taken into account during design; and
e. Any new or emergent technology communication devices or collaboration tools.

7.4. Monitored Systems and Applications

To help designers understand operations, the functional and technical requirements are operationalized during the design phase. These include considerations such as; which systems and applications require monitoring, display, the control and reporting functions of each work position and the application and functions required on the video wall.

The nature and type of systems and applications will vary, depending on the operational requirements of the SOC. The following is a generic list of applications which should be considered when developing the SOC design:

a. Electronic Access Control Systems;
b. Client Service Applications such as ID Card Production Equipment (if required);
c. Intrusion, Perimeter, Duress and Other Alarm or Event Capture and Display Systems;
d. Primary and/or Secondary Fire Alarm Annunciation Systems;
e. Elevator Control Systems and Elevator Call Response Systems;
f. Radio Systems;
g. Desktop Productivity Applications (e.g., email, word processing, spreadsheets, presentations, collaborative communications systems,);
h. Security Domain Applications (e.g., human resource systems, corporate intranet, timesheet systems, security incident reporting, scheduling);
i. Computer Aided Dispatch Systems and Applications;
j. Visitor and Contractor Management Systems;
k. Security Intercom Systems;
l. Emergency Notification Systems;
m. Emergency or Secure Phone Lines;
n. Video Wall Control Systems;
o. Audio Control Systems;
p. Cable Television Tuners and Controllers (hardware units or software applications);
q. Audio Recording and Playback Systems;
r. Keybox Control Applications;
s. Application Sharing from OGDs (e.g., police, fire, ambulance); and
t. CAD links with other police services.

7.5. Consoles

Consoles refer to the furniture on which the Operator Workstations are affixed. Typically, consoles provide a work surface, a structure on which to mount video monitors, power and audio/network communications management as well as video connectivity. This may or may not house computer workstations and other technical equipment. Regardless, in the design and selection of consoles, the following should be considered:

a. All operator-machine interface equipment (i.e., console) should travel vertically with the upper console section in a safe and smooth fashion. The operator should be able to safely and comfortably operate and maintain all equipment from fully seated to fully standing positions. The sit/stand console will usually contain an electric mechanism and have continuous height adjustment capability. Consoles should be comprised of a fixed base, motorized work surface and/or monitor mounts with keyboard support to achieve full sit-stand functionality. The monitors should move in tandem with the work surface and ensure that no pinch points exist in the structure. All controls should be within easy reach of the operator and not located in positions where they can be damaged by chairs, people or other near movable objects;
b. The console should be designed so the operator can sit or stand comfortably and comply with accepted Human Factors of Design and applicable ergonomic standards including ANSI/BIMFA, CSA and ISO;
c. In support of the installation, the console should be constructed in a modular fashion such that future requirements can be accommodated and defective parts can be replaced quickly;
d. Console parts and pieces (or modules, if so designed) should be able to be moved through normal single door openings;
e. The consoles should have a cable management system to allow for easy, structured installation and rapid modifications. The console cable management system will secure all cables running vertically or horizontally throughout the system preventing disconnection when the work surface is raised or lowered. Sufficient power bars and outlets should be provided for each console. These power bars would be used for technology such as the video monitors, CPUs, console actuators and radio system transformers;
f. The console should be equipped with a personal environment control system to provide local control over the user's environment, including circulating air and leg/foot warming and ventilation diffusers which are directionally adjustable;
g. Each operator console should be supported by a sufficient number of power circuits (ie. 15 Amp120V). Each power circuit should be provided with two duplex sockets immediately below the console location, ideally under the raised floor (if used). Console power bars (if used) should have sufficient length to reach the outlets;
h. Each operator console should have an ergonomic chair, space for binders and reference materials, a writing surface and a uniform layout;
i. Each console should be equipped with a door release to remotely unlock the doors without leaving his/her post. This release can often be provided as a hard-wired button or a software icon; and
j. Each console should be equipped with USB charging outlets and 120VAC auxiliary power available to the operator for ad hoc charging and electrical appliance use.

7.6. Operator Workstations

Operator Workstations are defined here as the technology affixed to and available from each console position. Each operator workstation should be defined by the designers in terms of the function to be provided/executed from that work position as well as the technical systems and communications capabilities required to perform that function. Considerations include hardware, software, telephony, user interfaces, and other forms of communications. Following are guidelines to be considered in the development of technical and operational strategies for the operator workstations.

a. Number of workstations required, including any redundancy;
b. Primary function carried out at each workstation (e.g., video monitoring, dispatch, intrusion alarm monitoring, social media monitoring);
c. Number and nature of security applications to be available at each workstation, such as: electronic access control, intrusion alarm monitoring, security video cameras, security intercom, telephone with TTY/RTT capability, computer aided dispatch, radio communications, CATV;
d. Number, size and configuration of on-console monitors, including primary, secondary and ad-hoc content to be displayed on each monitor;
e. Workstation mount strategy – in-console vs. in rack in Equipment Room;
f. Combined Keyboard-Video-Mouse (KVM) controllers (if required);
g. Video from workstation to video wall – for example, any workstation to anywhere on the video wall;
h. Intercom master station;
i. Telephone; and
j. Other systems.

7.7. Video Wall

The Video Wall provides a centralized display of data (video, alarms, events, CATV and EMT Feeds) for all members of the SOC operational team, as well as supervisors, management and other parties who may be present during events or crises. The addition of a video wall greatly enhances overall situational awareness in the SOC. The Video Wall display is an important tool to provide all staff with situational awareness of the 'business of the day' through camera call-ups relevant to the planned and unplanned activities within the area of responsibility. The Video Wall will support procedures regarding the sharing of video, intrusion, cable TV or desktop applications that an operator is viewing at his or her console thus allowing other operators to assist in a team effort with the issue being addressed. The following are general guidelines in the selection, positioning and use of a video wall in the SOC:

a. Using the available Wall Space and floor-to-ceiling space, a video wall consisting of a number of monitors (or an array of monitor cubes) will be designed. Monitor solutions providing for maximum viewable area with minimal frame visible in the field of view should be designed at a time closest to implementation to ensure that the most current technology is provided;
b. The means of displaying content on the video wall should be flexible. While each organization will select the information of most importance to achieve situational awareness, content which may be provided on the video wall includes:

- Security Video
- GIS Mapping Systems;
- Access Points Video and Systems;
- Intrusion and Perimeter Alarms;
- Technical and Other Events;
- CATV;
- Live Feed News Channels; and
- Emergency Layouts;

c. Consideration for inputs and positioning onto the Video Wall can be done through the use of a touchscreen video wall user interface that can be installed onto the Desktop PC at each of the Operator and Supervisor Consoles or from the console screens directly;
d. Viewing of video on the video wall should be generally situational. Pre-set views should be selectable based on the shift's operational business. Alarm-related response and the display of individual camera images as the personnel assigned to the SOC are often the primary responders for all security and life-safety events;
e. The video wall should also be able to support the configuration of a number of pre-established emergency scenarios that, when selected, display a pre-defined set of cameras on a predefined array of images on the video wall. The specific array definitions can be developed during the concept of operations and detailed design phases of the project; and
f. Audio capabilities will typically be provided for the Video Wall so that the operators can receive audio alerts, alarm sounding, dispatch audio, CATV and audio with video cameras from each of their work positions.

7.8. Supporting Business Machines

The SOC Control Suite typically requires office business machines to support the day-to-day operations of the SOC. Business machines installed in the SOC will vary based upon the need but should include, heavy-duty printer, fax (perhaps a secure fax), scanner, photocopier, and shredder (sufficient for the categorization of material). If a secure fax is required, sufficient space, location and security containers must be considered.

7.9. Audio/Video Logging and Recording

While the collection of audio and video recordings for evidentiary and performance improvement processes differ with each organization, the recording of audio/video within the SOC is recommended. Departments should consider their individual requirements prior to beginning to collect recordings however if it is determined that recording is required or desired, the following sources should be considered within the SOC:

a. Audio recording capability to capture and store radio communications, VOIP and analog telephones, intercom master stations;
b. Departments may choose to record ambient video and audio communications in the SOC during emergencies. If this is the case, a notification light in the room should alert all occupants that this is occurring. Recording devices such as stand-alone microphones, or integrated components of CCTV security cameras can be installed

within the room for the purpose of recording the ambient communications; and

c. Playback of recordings should only be possible by a properly authorized operator workstation console (ie SOC Manager) however, outside the SOC Control Suite, typically only the supervisor has authorization. Playback authorization for operators should be limited to immediate requirements only where supervisors should have longer-term access.

7.10. CATV

Global and location situational awareness is improved by providing mass media news feeds through Cable Television Tuners. The number and type of tuners (ie IPTV, Cable Television, Digital Television, Streaming Services, etc.) will be defined during detailed design. CATV control capabilities should be defined and designed to meet the operating protocols of the organization (e.g., does supervisor have control, do all operators have control, which channels are blocked, where does audio control rest?). Following are specific CATV guidelines:

a. Departments may consider displaying CATV on the video wall. CATV feeds consisting of News Channels and other CATV feeds are displayed on any number of monitors however; the specifics will vary depending on requirement. The ability of the operator to select a particular CATV channel should be limited to those channels authorized by the supervisor. A supervisor would have the ability to select any channel however these selections should be limited to those authorized by the department;
b. Selection of the CATV channels can be done in different ways (typical TV remotes, through the use of a touchscreen CATV user interface, or from an operator workstation software application);
c. Speakers, sized and powered to meet the needs of the size of the room are typically placed at the front of the room (one on either side of the Video Wall); and
d. Additional speakers may be needed directly above each console and individual controls at each console are provided to the operators for these speakers.

7.11. UPS and Emergency Power

It is critical to have sufficient, sustainable power sources for the operation of the SOC, which must remain operational at all times. Therefore, appropriately selected and sized power systems should be provided. The following are minimum requirements related to power, technical power and emergency power:

a. Centralized or local UPS and back-up/emergency power should be provided to all security spaces, systems and equipment including lighting and HVAC;
b. UPS and Emergency power are required for the SOC computing, display, communications and networking equipment. This also extends to all sub systems including support and infrastructure, HVAC, network, mechanical, electrical, lighting, and other life-safety systems;
c. Sufficient UPS time should be calculated to allow the emergency power to be initiated, and to support a gentle shutdown of systems not supported by emergency power, or not required in an emergency power scenario;
d. The generator and fuel reserve should be sized to allow equipment to function for a

minimum amount of time, as defined by the organization (e.g., 24, 48, 72 hours);

e. Electrical circuits serving all equipment and systems for the SOC should be dedicated and not be shared with other building services; and
f. Electrical circuits serving equipment and systems for the scanning area operations should be dedicated and not be shared with other building services.

7.12. Mechanical Systems/HVAC/BMS

As described in Section 4.3 on Ergonomics, the quality and reliability of the air quality and temperature in the SOC is critical to ensuring high performance operations. Following are guidelines related the mechanical design of the SOC Control Suite space itself:

a. A separate Building Management System BMS, including HVAC system is typically specified for the SOC;
b. The air handling units serving the SOC should be separate from the main air systems of the building. Air intakes should not be located at grade level. Air intakes and exhausts should not be adjacent to each other;
c. For all areas, temperature should be adjustable between 21 degrees C and 23 degrees C in winter and 23 degrees C and 26 degrees C in summer. An independent temperature control is typically required for the SOC. Humidity should be adjustable between 25% and 65% RH. Pre-filters in the fresh air and return inlets use 75% to 90% arrestance filters; and
d. There should be filters on the discharge side of the heating and cooling coils;
e. HVAC ducting that perforates the building envelope should not exceed 620 square centimeters (96 square inches) in cross section. Ducting that exceeds this dimension should be equipped with security grillwork conforming to RCMP Secure Duct openings.

7.13. Infrastructure & Cable Requirements

Power and connectivity are required for all technical components and systems in the SOC. To meet electronic security requirements in the SOC, it is necessary for the project to provide security conduit, cable trays and pathways and associated cabling. In addition to functional requirements being met (i.e., pathways and electrical/data cabling), particular security features of the infrastructure systems should also be provided. In addition to industry best practices for the installation of infrastructure components, the following guidelines are of use:

a. All cable should be installed within a sealed EMT conduit system. However, it is also acceptable to install cable within a cable tray or cable trough if it is in a secure space (e.g., the SOC Control Suite, the Equipment Room, under the raised floor);
b. Where practical, security junction boxes should be locked and equipped with tamper-proof covers;
c. Junction boxes located in public or reception zones should be equipped with tamper sensors;
d. The Infrastructure design should meet the standards outlined as follows:
    - TIA/EIA #569 Standard for Pathways and Spaces
    - TIA/EIA #606 Standard for Labelling
    - TIA/EIA #607 Standard for Grounding and Bonding
    - TIA/EIA #568 Standard for Telecommunication Cabling

e. Sufficient infrastructure (cable trays, troughs and/or conduit) are needed between the adjacent equipment room and the SOC Control Suite itself;
f. All in-suite cable (i.e., cable between the equipment room and the consoles and video wall components) is typically provided by the contractor responsible for the implementation of the SOC consoles and technology; and
g. All cable will be required to meet equipment and manufacturer specifications and be coordinated with the design team.

7.14. Equipment Room

The Equipment Room (ER) serving the SOC Control Suite is typically located as close as possible to support the provision of power and technical connectivity. Considerations for the location, design and security of the room are as follows:

a. The SOC ER should be located adjacent to the SOC Control Suite so that power systems can control both the SOC Control Suite and the Equipment Room with both UPS and Emergency Power systems. It also means that connectivity performance between the ER and the SOC Control Suite can be maximized;
b. The size of the SOC ER should be sufficient to meet all technical requirements with at least 50% spare capacity for growth;
c. Design racking systems in the space so; sufficient circulation around the racks is maintained (at least 1.5m on all sides), they are seismically restrained to meet current codes and standards and that they support the computing, networking, connectivity and multi-media equipment (e.g., video wall processors);
d. The ER will require sufficient HVAC support to cool all of the equipment in the room. Designers will need to provide the project with heat/power loading information to guide the HVAC design;
e. The ER will require sufficient UPS and Emergency Power to support all of the equipment in the ER and the SOC;
f. A raised floor in the ER will greatly enhance the connectivity and power designs since the ER is adjacent to the SOC Control Suite;
g. Consider, in-room temperature, flood and humidity sensors;
h. Overhead cable trays should not impede access to all rack-mounted equipment, but should also provide service to all cabling;
i. The walls separating the equipment room from the SOC Control Suite should be required to meet a standard of SPC 85 at a minimum;
j. Manage access to the Equipment Room by an electronic access control system; and
k. Ensure to install or consider smoke detectors and a fire suppression system for the Equipment Room.

8. SOC Design and Implementation Standards & References

The following are industry and governmental standards and guidelines, which may provide SOC designers with additional support in defining functional and technical requirements, developing concepts of operations and concept or detailed designs:

- Treasury Board Secretariat Policy on Government Security, July 1, 2019
- Security Design – PWGSC Federal Office Building Standards
- Treasury Board of Canada: Accessibility Standard for Real Property
- National Building Code
- Provincial Building Codes
- RCMP Technical Security Branch Technical Operations Publication G1-031 Physical Protection of Computer Servers
- RCMP Technical Security Branch Technical Operations Publication G1-024 Control of Access
- RCMP Security Systems Branch Security Guide Publications SSB/SG-21 Construction of a Special Discussion Area, August 1988
- RCMP Technical Security Branch Technical Operations Publication SG-29 Guidelines for Guard Services, April 2001
- RCMP Technical Security Branch Technical Operations Publication G1-006 Identification Cards/Access Badges
- RCMP Technical Security Branch Technical Operations Security Control Centre Space Requirements G1-013, September 2006
- RCMP Technical Security Branch Technical Operations Guide to the Preparation of Physical Security Briefs G1-005, January 2000
- ASIS International Facilities Physical Security Measures Guideline, 2008
- ASIS International Threat Advisory System Response Guideline, 2008
- ISO11-064-1 through 7 Control Centre Design Standards
- CAN/ULC-S301-09 SIGNAL RECEIVING CENTRE BURGLAR ALARM SYSTEMS AND OPERATIONS
- CAN/ULC-S304-06 SIGNAL RECEIVING CENTRE AND PREMISE BURGLAR ALARM CONTROL UNITS

9. Promulgation

Reviewed and recommended for approval

I have reviewed and hereby recommend GCPSG-003 (2021) – Security Operations Centre Design Considerations Guide for approval.

Nattress,Shawn Thomas,000302786

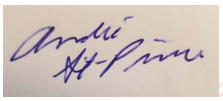
Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2021.08.12 11:04:43 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-003 (2021) – Security Operations Centre Design Considerations Guide.



Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2021.08.12 11:43:35 -04'00'

André St-Pierre,
Director, Physical Security
RCMP

Date