

# Conducting Security System Site Surveys

Written By:  
Harold C. Gillens, PSP, CFC, CHS-III



Quintech Security Consultants, Inc.  
102 Sangaree Park Court  
Suite 4  
Summerville, SC 29483  
[www.quintechengineering.com](http://www.quintechengineering.com)

## CONDUCTING SECURITY SYSTEM SITE SURVEYS

### I. BACKGROUND:

In the aftermath of September 11, 2001, Federal, State and Local authorities all turned their attention to assessing their security posture. Each of them began making the necessary adjustments to ensure proper levels of security. However, in their attempt to do so, many organizations discovered that they possess a multitude of different systems and security technologies. At that point of discovery, it was now up to someone to determine the best security technology required to move them forward in their quest to provide optimum security for protection of personnel, facilities, and other critical assets.

Security managers often find out quickly that determining their “AS-IS” condition is the first step in obtaining its security objectives. To do so, security managers want to know what type of systems are currently in place, their functional status and expansion capability, and their past performance and reliability. In addition, they need to obtain information on the current security infrastructure and facility resources needed to support its operations. The usability of current infrastructure plays a major role in the ultimate decision of maintaining items currently in place or migrating to a new system. The IT Network as a security infrastructure has become both a positive and negative for organizations.

The ultimate objective for security managers is to develop recommended solutions for increase security posture and to define and implement a strategy to get them to their newly defined “TO-BE” state.

### II. PURPOSE:

The purpose of this White Paper is to provide organizations seeking to increase their security posture with a list of task areas required to successfully accomplish an Electronic Security System (ESS) Site Survey of their campus-wide environment and to assist them with guidelines for selecting a qualified Security Consulting Firm.

### III. STATEMENT OF NEEDS:

An ESS Site Survey should include identifying and evaluating the “AS-IS” condition of existing security systems used by the organization to protect against unauthorized access, provide intrusion detection, and to provide closed circuit television surveillance of critical areas. Recommendations should be developed with a strategic understanding of the on-going capital improvement projects. Considerations for the out-years should be identified as “TO-BE” upgrades and should be incorporated as part of the site survey report. Recommendations and solutions for modifications and upgrades should be developed with an understanding that all processes, systems, and resources must be integrated to provide a comprehensive campus-wide security management plan.

Within the site survey report, milestones should be identified for the ESS upgrade that is compatible with the organization’s capital improvement plan and the levels of protection consistent with the protection of key assets and facilities.

The site survey should closely follow the process as outlined in the task areas below:

**Task Area 1 – Conduct Site Survey:** Addresses physical security and access controls as the first line of defense for protecting the organization's asset. The survey should include, as a minimum, each of the following.

- Perimeter and interior access control
- Mail, Packages and Delivery systems
- Traffic and barrier planning
- Parking
- CCTV surveillance
- Intrusion detection
- Response capabilities

### **Site Survey Process**

- a) Hold an in-brief with site personnel to outline survey goals.
- b) Hold discussions with site personnel to discuss issues such as:
  - Operational procedures and security requirements
  - Organization structure, roles and responsibilities
  - Available and planned resources
  - On-going or planned security projects
  - Real or perceived threats not yet guarded against
  - Past incidents (types, impact, resolutions)
- c) Survey each facility to gather information that includes at a minimum, the following:
  - 1) Access Control System
    - Locate and document all access control systems. Determine equipment type and operating condition.
    - Locate and document all access control system field panels. Note adherence to good installation practices and fire safety standards.
    - Locate and document all access control card readers. Determine reader type and operating condition.
  - 2) Communications Backbone
    - Examine and document the type and condition of existing wiring and cabling.
    - Determine the adequacy of existing infrastructure to handle future access control security requirements.
    - Examine adequacy of existing telephone lines.
    - Examine existing network Topology.
    - Examine and document current deployed communications encryption.
    - Note adherence to applicable ANSI, EIA and TIA commercial telecommunications standards.

- 3) Access Control Monitoring Control & Display Equipment (MC&DE) and Badge Station
    - ❑ Examine the MC&DE and document the salient characteristics, i.e., Operating System Software and Version; MC&DE System Software and Version; database type, etc.
    - ❑ Document each access control system's architecture.
    - ❑ Examine the systems capacity, i.e., maximum number of card readers, card holders, access points, etc.
    - ❑ Examine historical records to determine the system's activity.
    - ❑ Examine and document the system's database structure and data distribution methodology.
    - ❑ Examine and document the systems integration to existing intrusion detection and fire alarm systems, and Closed Circuit Television (CCTV) systems.
    - ❑ Document the existing concept of operation for all access controls systems installed and monitored in the facility.
    - ❑ Examine and document the badge station set up and concept of operation.
    - ❑ Examine and document the methodology for system back-up.
    - ❑ Examine and document the site's methodology for disaster recovery.
  - 4) General Facilities
    - ❑ Examine and document the adequacy of emergency back up power.
    - ❑ Examine and document the adequacy of UPS in assuring continuity of operations in power fail situations.
    - ❑ Survey facility to identify areas that are now vulnerable or may present a potential of becoming an at risk area.
    - ❑ Compile building drawings and sketches, if available, to be used in generating proposed equipment layouts.
- d) Hold an out brief to sum up the site survey findings.

**Task Area 2 — Technologies Evaluation & Analysis:** Assist in identifying and recommending security products and applications to upgrade security systems and technologies. Considerations should include:

- Security system development, which may be integrated with the existing and new infrastructure – incorporating security system servers, security management system software, advanced processing alarm and card access controllers, control panel and lock power supplies, operator, administrative and identification badging workstations, identification badge printer, report printer, CCTV matrix switcher, CCTV cameras, duress intercoms, intercoms, and digital video recorders (DVR).
- Integration criteria used to incorporate/installed card readers, alarm sensors, and security cable infrastructure to the new and existing facilities as identified and approved by the educational institution's committee, evaluating the recommendations of the final assessment report.
- Personal Identity Verification (PIV)/badge system to be used as part of the overall security management system. The PIV should be able to accommodate smart card technology.
- The contractor should also make recommendations and consider perimeter systems, barrier controls, and traffic plans to support the facility development efforts.

**Task Area 3 – Prepare Site Survey Report:** Utilizing the information obtained during the site survey of each facility, the contractor will develop a Security Assessment Report. The report should outline all the findings of the surveys and make recommendations for upgrading existing intrusion detection, CCTV, and access control systems. These recommendations may include the integration of additional equipment, training, procedures, and safeguards required to maintain and/or increase the client's security posture and to further mitigate identified vulnerabilities and perceived threats documented during the survey phase. Recommendations may include:

- Installation and/or upgrading of access control and alarm monitoring equipment
- Installation of additional CCTV cameras and/or relocation of existing cameras
- Institution of physical security counter-measures (vehicle barricades, fence lines, metal detectors, etc.)
- Upgrade of indoor and outdoor lighting
- Creating or modifying existing security policies and procedures
- Potential reorganization of current organizational structure
- Recommendations for continuity of operations in a crisis situation
- Designing, installing and integrating the most efficient and cost effective Integrated Security Management System to meet the client's requirements.

The intent of the organization's security report is to highlight the findings of the assessment and briefly describe recommended security improvements required to strengthen the security posture of the campus environment. A second goal of the report is to highlight ways of decreasing potential liability exposure.

#### **IV. SECURITY PROFESSIONAL'S QUALIFICATIONS:**

The first step in selecting a security consultant or consulting firm should be to verify its true independence of manufacturers and system integrators. The benefit in doing so is to ensure that the consultant is working on behalf of the organization and is not there to deliver any preconceived solution. It is important to remember that the selected security professional could be a part of your in-house staff. In-house security professions may also provide a non-bias and independent view of one's security needs.

The next step is to verify the company's or consultant's credentials with respect to the specified task areas. The qualified company or team should have both physical and information security professionals with associated professional certifications. The company or consultant should also possess senior level engineering and/or project management skills. Physical security professionals will typically have the following certifications:

- Certified Physical Security Professional (PSP)
- Certified Protection Professional (CPP)
- Certified in Homeland Security (CHS)

Information security professionals will typically have the following certifications:

- Certified Information System Security Professional (CISSP)
- National Security Agency's Information Security Assessment Methodology (NSA-IAM)

It should be emphasized that professional experience may be more important than credentials and those with experience can bring to bear industry's best practices.

The contractor should also provide a Project Manager for the security assessment task. This individual should have:

- Proven experience in managing security programs and conducting analysis, studies, and assessments.
- Proven capability working in security management with threat analysis and vulnerability assessment experience.
- Demonstrated experience as a security consultant developing security programs, integrating security systems and products and managing federal government security engagements.
- Experience supporting the national efforts engaged in the continuity of government and continuity of operations planning.

#### **V. NEXT STEP (FOLLOWING REPORT DELIVERY):**

The Security Assessment Report is the resulting document from the site surveys and all task area performance. Following the approval of the security recommendations, a Statement of Work (SOW)/Request for Proposal (RFP) should be developed that consist of descriptive information based on all approved recommendations; request for contractor support in the development of policies, procedures and support of the system design process.

Along with the new policies and procedure development, an Installation Design Plan (IDP) should be developed detailing the overall system configuration for the organization's campus-wide security upgrade. The typical duration for an IDP development and approval could take approximately 60 to 90 days for task completion. The development process contains, at minimum, a 30%, 60%, and 100% design review with all stakeholders. To speed up this process, the end-user may agree to have the system integrator use the approved 60% design package to conduct procurement and installation. The as-built drawings will then be completed using red-lines generated during the installation period. By doing so, the end-user may be able to reduce the design time by 30 to 45 days getting to the installation phase much faster.

*(Stakeholders including, but not limited to, IT Department, Safety & Protective Service/Physical Security, and others to be identified by the executive staff.)*