Specialists in IP and digital networking solutions
Closed Circuit Television Systems
Integrated Security Systems
Access Control Systems
Physical Security
SITO approved Training
IT and Network Security
Electronic Countermeasures
Integrated Management Systems
Business Continuity Management

Tel: +44 (0) 1604 407 819
Fax: +44 (0) 1604 407 846
Company Profile.

The Company was formed to bring together experienced management professionals of known quality to provide expert, impartial and confidential consultancy services to the Public Sector, Industry, Banking, Government Departments, Military and Police Authorities in the UK, Europe and the Middle East.

As a matter of policy, we maintain the strictest impartiality. The Company has no allegiance to or commercial links with any manufacturer, distributor, or installer. The only interests considered are always, exclusively, those of the particular Client for whom we are acting.

All Directors and Associates have agreed to abide by the following obligations and conditions:

- To maintain a high standard of work and to act with integrity and impartiality solely in the interests of the client.
- To maintain confidentiality of information specific to the business of the client.
- To accept only those assignments, which we consider ourselves competent to carry out personally and/or with the assistance of others, who in our judgement are similarly competent and who comply with the requirements of this Code of Conduct.
- To disclose to the client any personal or financial interest, or any other significant circumstances that might involve a conflict of interest.
- To agree with the client in advance the objectives and scope of the assignment and the fees or fee basis and other terms and conditions. In the event of subsequent changes to the original brief, to submit a revised proposal to the client for his acceptance.
- To maintain effective communication with the client, and to submit appropriate reports and documents.

ASC Member,
Association of
Security Consultants
The Services.

We provide a comprehensive and bespoke service that incorporates effective security measures and realistic contingency planning that work with the needs of the organisation and its employees for the corporate and public sectors. The Services provided are divided into several modules as described below:

Risk Assessment, Contingency and Risk Management.

Vulnerability and security assessments involve a detailed and independent evaluation to provide a realistic overview of the Company’s strength and weaknesses. In Management terms, this is similar to a S.W.O T (Strength, Weaknesses, Opportunities, and Threats) Analysis. We shall examine both internal and external threats, prioritise for their likelihood, and review damage potential. Practical and realistic advice is provided on additional measures that can be implemented to enhance and compliment the existing systems.

Defining the Operational Requirement.

This will include discussions with the Company’s Security, Financial, and Operational staff. The operational requirement will define the broad requirement for a business solution based on budget and operational restrictions. During this phase, we shall undertake several stages, which include the following:

Designing out the risk & Specification Setting
As the most critical stage of the entire process, the design will combine the Client’s needs with the capability of the resource, whilst remaining within the constraints of any budget requirements. From there, the best resource components will be chosen to ensure that the solution operates as per the design criteria. This will evolve into a Specification for use in any tendering process. We shall cover all aspects of security including physical, electronic, and man guarding.

Tendering Process
We shall prepare the technical specification and operating requirements of the tender documentation to reflect the Client’s own procedures, in terms of contractual conditions, quality management and health & safety systems.

Tender Assessment
A technical evaluation of the tenders will ensure that the Tendering Companies have fully understood the specification and that they have returned a compliant bid. We shall make our recommendations to the Client as to the best technical bid.
Project Management.

GDC shall attend site meetings and carry out site progress audits to ensure that the works meet the Client’s expectations. We shall also be available to assist with any technical queries that may arise during the course of the contract. In addition, we will undertake the following activities:

**System audits.**
On completion a detailed check, to include night and full operational tests, will be made to ensure that the systems are fully compliant and meet with the Client’s requirements. We will ensure that the Contractor leaves a complete set of documentation on site, which will include system drawings, schematics, maintenance manuals, and operation guides.

**Handover of System**
GDC will ensure that handover of the entire system is in accordance with the specification. Additionally, we can monitor any client training. The Contractor will not receive any payment until full compliance.

**Processes and Procedures.**
Writing the procedures in line with the various British Standards can be undertaken to meet the Customer’s requirements.

Business Continuity Management.

Business Continuity Management (BCM) is the process of anticipating and managing incidents that will affect the critical functions and activities of an organisation, ensuring an operational response in a planned and rehearsed manner to a pre-determined acceptable level. A summary of the methodology is as follows:

**Business Impact Analysis.**
In order to ensure that the business ‘down time’ is kept to the absolute minimum, we shall undertake a Business Impact Analysis to establish a realistic and practical recovery programme.

**Implementation of Measures.**
The Management Team may implement counter-measures, which could include employee awareness training and the preparation and implementation of a crisis management team. We shall oversee the full test and evaluation of the contingency plans.

**Reviews and Updates.**
Once the contingency plans are in place, constant and regular reviews form an integral part of the Business Continuity Management Process.

Tactical Evaluation.

After the implementation of the various components that form the complete security solution, it is necessary to carry out covert tactical evaluation of the systems. We will attempt to find a weakness in the system and try to exploit it to see if the existing processes and procedures work. This is normally done with the full knowledge and backing of the Company’s Board of Directors.
**Specialist Services**

Due to the increased demands by its Customers, ODCL have added the following modules to its range of offering.

*Electronic Countermeasures.*
We will undertake the technical sweep of Boardrooms and conference rooms to detect hidden listening and recording devices. In the case of new buildings, this process should be undertaken as soon as cabling work is finished, before occupation of the building and on a regular 6 monthly basis thereafter or prior to specific meetings where confidentiality is paramount.

A survey by the National Computing Centre for the DTI found that two fifths of all sites surveyed reported a significant information security breach during the previous two years, and half of these thought that they could have taken steps to prevent it. We can help implement a system that will meet the current standards and suit the customer's needs.

*Health & Safety at Work.*
Company Directors have a legal requirement to take care of the Health and Safety of all their staff and others who might visit their premises or be exposed to their work i.e. whilst installing a product. A Company must be aware of all changes to the legislation that affects them, review their operations and documentation, and revise them when necessary. We can implement the complete standard, and keep the Customer abreast of Policy changes by using our Health & Safety Update Scheme. In addition, we can assist with Construction Design Management (CDM) Regulations, OHSAS 18001 and 18002 systems.

*Integrated Management Systems.*
An Integrated Management System will combine one or more management systems (i.e. BS EN ISO 9000:2000 and environmental systems) into an integrated system and set of documentation. This eliminates the duplication of work and documentation for common system elements like auditing and document control. This provides the Management of a Company with improved efficiency and potential savings.

*Training.*
The Company can provide a wide variety of training courses either in-house or at our own SITO approved training facility. The courses are customised to the requirements of particular Clients, and graded from basic to middle management level.

*Outsourcing.*
The Client can retain our Services to provide all or some of the above on a full or part-time basis. We would work in partnership with the Company’s Management Team to provide a cost effective outsourced specialist service.
IT Security Reviews

GDCL provides 3 levels of penetration testing of an IT network environment by simulating everything a “Hacker” or “Cracker” would attempt, to gain access to a system and information.

**External Hacking.**
The process has nine steps detailed below.

- **Foot printing**
  a. To target address range, namespace acquisition, and information gathering.
  b. To profile the organisation security posture.
  c. To obtain an overall picture of the environment.

- **Scanning**
  a. To identify and list all services and access points
  b. To look for the most promising avenues of entry.
  c. This is the passive investigation.

- **Enumeration**
  a. This is an invasive probing, when the attack begins.
  b. Begin identification of user accounts.

- **Gaining access**
  a. Enough data has been gathered at this point to try to gain access.
  b. Password guessing and brute force cracking giving access to services.

- **Escalating privilege**
  a. Get administrator or system access

- **Pilfering**
  a. Information gathering to access other trusted systems.
  b. Gathering information for information’s sake

- **Covering tracks**
  a. Once total ownership is achieved, remove all indications of entry.
  b. Removal of log files and shutdown of logging system.

- **Creating back doors**
  a. Create hidden shortcuts into the systems for future use.
  b. Also used to hide the originator of attacks on other systems.

- **Denial of service**
  a. Turning services off or use systems as a jump off point to turn other systems off (DOS)

**Security Audit.**
This stage includes the above steps and requires the cooperation of the Company. GDCL will undertake a complete audit of the systems as System Administrator.

**Internal Penetration Testing.**
Since 82% of all penetration is carried out by or with the assistance of an insider, GDCL will set the entire internal security policy from passwords upwards.

**Report**
GDCL will detail the technique and the tools used, highlight the information discovered and recommend how to fix the problem areas.

**Professional Experience - Summary.**
Consultants

Stuart Kerstin  Member of the American Society of International Security (A.S.I.S), Member of the Association of Security Consultants (A.S.C) and the Institute of Directors (I.O.D).
Brian Barratt  Member of the World E.O.D Foundation and the Institute of Directors (I.O.D)
Tony Tesar  Member of the World E.O.D Foundation, Member of the Business Continuity Institute.
Robert Kemp  Member of the Institute of Mechanical Engineering (M.I.Mech.E), Member of the Institute of Operations Management (M.I.O.M).

Synopsis of work undertaken.

Channel Tunnel Maintenance depot.
120 cameras with video motion detection located around a 5kms perimeter fence fitted with a fibre optic fence mounted system. This system was treble knocked with the video motion detection system as well as passive infrared detectors. An access control system was also installed. All the video, data and audio signals were transported to 2 control rooms via fibre-optic cabling. We undertook the system design and project management of the project. Project value £3M.

Royal Air Force sites.
To carry out the installation of three high-speed target acquisition video camera systems installed at the end of runways to work in very low light levels and in the thermal imaging range. These cameras were used to track jet fighters coming in to land to check the undercarriage was down. This involved the complete system design and the product design implementation of specialist software to carry out the task. All signals had to be carried over 7kms of fibre-optic cables. Project value £500k.

Mersey Rail.
To carry out the system design and project management of a complete redundant fibre-optic ring suitable for the transmission of 200 cameras as well as data and audio channels. This was done using single mode fibre and a drop and insert topology based on multiplexing 16 video channels down 1 fibre. All the work had to be carried out at night and special attention had to be given to Health and Safety problems.


The above are only a sample of the work that we have undertaken. Unfortunately, most of our work is classified or sensitive in its nature, which means that we are unable to provide full details to anyone.
Customer's List

- Sun Microsystems Limited - Approved supplier status
- Energis Plc
- Nissan Design Europe Ltd
- Industrious Limited - Partnership arrangement
- T.N.T
- Travis Perkins
- B.R.E/L.P.C
- London Bus Services Limited - Approved supplier status
- The National Forest
- South Derbyshire District Council
- JBR Recovery Ltd
- Acclaim Corporate Events Limited