Business Management System

Integrated 9001:2015 & ISO 27001 2013

Table of Contents

Control Document

8.3.2 Design and development planning
8.3.3 Design and development inputs
8.3.4 Design and development controls
8.3.5 Design and development outputs
8.3.6 Design and development changes

8.4 Control of externally provided products and services
8.4.1 General
8.4.2 Type & extent of control of external provisions
8.4.3 Information for external parties

8.5 Production and service provision
8.5.1 Control of production and service provision
8.5.2 Identification and traceability
8.5.3 Property belonging to customers or external parties
8.5.4 Preservation
8.5.5 Post delivery activities
8.5.6 Control of changes

8.6 Release of products and services
8.7 Control of non conforming process outputs, products or services

Clause 9 - **Performance evaluation**
9.1 Monitoring, measurement, analysis and evaluation
9.1.1 General
9.1.2 Customer satisfaction
9.1.3 Analysis and evaluation

9.2 Internal Audit

9.3 Management Review

Clause 10 - **Improvement**
10.1 General

10.2 Non conformity & corrective action

10.3 Continual improvement

1. INTRODUCTION

This document is the Business Management Manual (the Manual) of SECFORCE LIMITED and for the purpose of this manual will be referred to as 'SECFORCE'.

The Manual is the property of SECFORCE and is a controlled document.

The purpose of the Manual is to provide an overview of SECFORCE, the activities it carries out and the quality standards of operation it conforms to.

It is not designed to act as a procedures manual, although it does carry information about where procedures information is located and the detailed information on documentation requirements for the procedures required by the respective standards.

This Manual is designed to meet the requirements of ISO9001:2015 and ISO 27001:2013 and any standard which adopts the Annex SL structure

1.1 THE ISSUE STATUS

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this Manual.

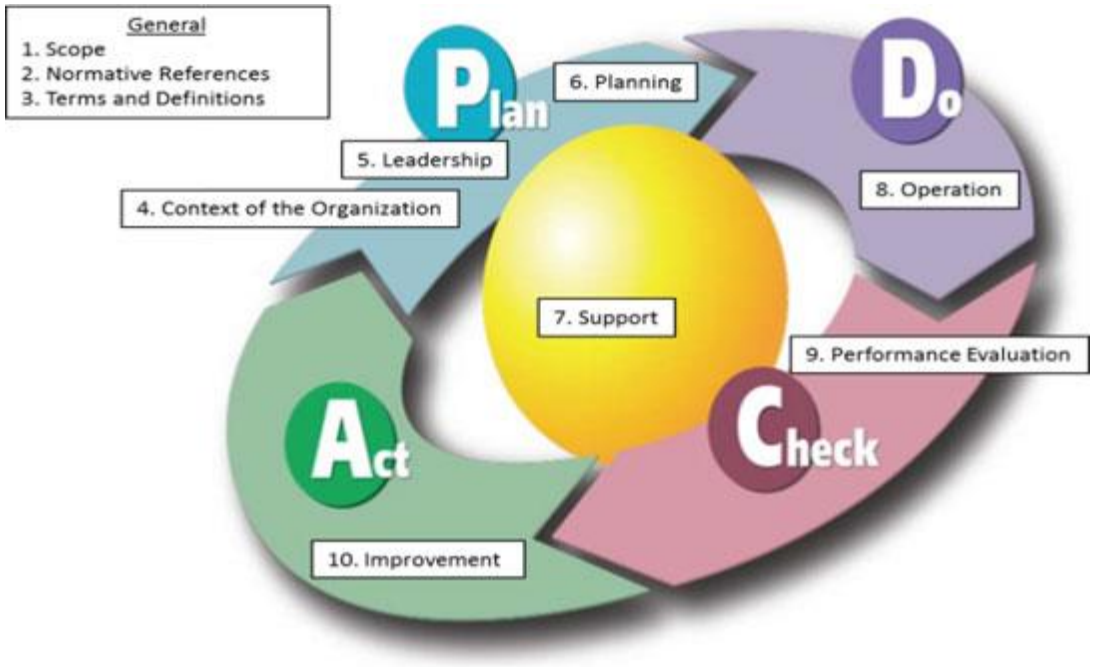
When any part of this Manual is amended, a record is made in the Amendment Log shown below.

The Manual can be fully revised and re-issued at the discretion of the Management Team.

Please note that this Manual is only valid on day of printing.

Issue	Issue Date	Additions/Alterations	Initials
0.1	09/01/2017	ISMS Manual First Draft	ES
0.2	July 2017	Revision and minor amendments	RM
0.3	December 2017	Amendments to 4.2, 6.1.12; added section 8.3 and 8.4	ES
0.4	January 2018	Updates to 4.1, 4.2	ES
1.0	July 2018	Revision and minor amendments	RM

1.2 PLAN-DO-CHECK-ACT Model



1.3 QUALITY and ISMS POLICY

It is the policy of **SECFORCE** to maintain a quality system designed to meet the requirements of ISO 9001:2015 & ISO 27001:2013 in pursuit of its primary objectives, the purpose and the context of the organisation.

It is the policy of **SECFORCE** to:

- give satisfaction to all of our customers and other stakeholders and interested parties whenever possible, meeting and exceeding their expectations;
- make the details of our policy known to all other interested parties including external where appropriate and determine the need for communication and by what methods relevant to the business management system. These include but not limited to customers and clients and their requirements are documented in contracts, purchase order and specifications etc;
- comply with all legal requirements, codes of practice and all other requirements applicable to our activities;
- the reduction of hazards, prevention of injury, ill health and pollution;
- provide all the resources of equipment, trained and competent staff and any other requirements to enable these objectives to be met;
- ensure that all employees are made aware of their individual obligations in respect of this quality and information security policy;
- maintain a management system that will achieve these objectives and seek continual improvement in the effectiveness and performance of our management system based on "risk".

This quality and information security policy provides a framework for setting, monitoring, reviewing and achieving our objectives, programmes and targets.

Customer service is an essential part of the quality process and to ensure this is fulfilled, all employees receive training to ensure awareness and understanding of quality and information security and its impact on customer service.

To ensure the company maintains its awareness for continuous improvement, the business management system is regularly reviewed by "Top Management" to ensure it remains appropriate and suitable to our business. The Business Management System is subject to both internal and external annual audits.

Scope of the Policy (ISMS Only)

The scope of this policy relates to use of the assets and computer systems operated by the company at its office in London, in pursuit of the company's business of providing security consultancy services to its clients.

2. OVERVIEW OF THE ORGANISATION

SECFORCE Limited, established in 2008, is a UK based company formed by the industry leading security experts with the aim of delivering quality and comprehensive information security consultancy. As a vendor independent firm SECFORCE provides impartial security advice in line with the business requirements and providing solutions with measurable returns.
SECFORCE is a dynamic company passionate about security, analysing the latest security trends and contributing to the industry with open source software and security talks.
Its security consultants are creative, well respected in the field and contribute to our client's success not only with their broad technical knowledge, but also with understanding of organizations processes and procedures.
SECFORCE approach to security consultancy aims to be one to one, comprehensive, realistic and suitable for our client's necessities. We offer a unique combination of technical and business experience that allows us to deliver just the solutions that our clients need.

2.1 SCOPE OF REGISTRATION

Provision of IT security consultancy services

Top Management
Rodrigo Marcos, 19/07/2018

3. OBJECTIVES

We aim to provide a professional and ethical service to our clients. In order to demonstrate our intentions, Our Management Team will analyse customer feedback data, internal performance data, financial performance data and business performance data to ensure that our Quality Objectives are being met.

Quality

We have identified the following Quality Objectives

- We will endeavour to deliver our services to specification, on time and to the price quoted
  This is measured via the SECFORCE Scheduler Administration tool (http://172.16.16.161:82/admin/) which includes projects' timelines, objectives and date of start and delivery.

- We will conduct our business in an ethical and professional manner
  This is measured by the number of positive feedback received by the clients, recorded on http://172.16.16.161:82/admin/feedback/feedback/

- We will endeavour to satisfy our clients' requirements and get things right first time. Should we make a mistake, we will admit it and rectify the situation as quickly as possible.
  This is measured by the feedback received by the clients, recorded on http://172.16.16.161:82/admin/feedback/feedback/

Information Security

SECFORCE's ISMS Objectives are as follows:

- Objective 1: Existing services - SECFORCE will continue to deliver its services within a secure environment, measured by the number (or lack) of security incidents recorded per year

- Objective 2: Development - SECFORCE will conduct annual risk assessments to ensure that risk to information in the care of SECFORCE is minimised or eliminated, measured by the number of risks and their severity.

- Objective 3: Improvement – SECFORCE will improve and streamline its processes based on the interested parties' satisfaction and feedback, measured by the feedback received by the clients, recorded on http://172.16.16.161:82/admin/feedback/feedback/

4. CONTEXT OF THE ORGANISATION

4.1 Understanding the organisation and its context

The context of the organisation is demonstrated within this Business Management System and all associated processes connected with the services / products offered.

The legal legislation / regulatory compliance to the service / products offered are listed below.

Data Protection Act 1988	https://en.wikipedia.org/wiki/Data_Protection_Act_1998
Freedom Of Information Act 2000	https://en.wikipedia.org/wiki/Freedom_of_Information_Act_2000
The Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000	http://www.legislation.gov.uk/uksi/2000/2699/contents/made
The Electronic Commerce (EC Directive) Regulations 2002	https://en.wikipedia.org/wiki/Electronic_Commerce_Regulations_2002
Computer Misuse Act 1990	https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990
The Electronics Signatures Regulations 2002	https://en.wikipedia.org/wiki/Electronic_Commerce_Regulations_2002
The Telecommunications (Data Protection & Privacy, Direct Marketing) Regulations 1999	http://uk.practicallaw.com/1-100-9513
The Consumer Protection (Distance Selling) Regulations 2003	https://en.wikipedia.org/wiki/Consumer_Protection_(Distance_Selling)_Regulations_2000
Regulation of Investigatory Powers Act 2000 (RIPA)	https://en.wikipedia.org/wiki/Regulation_of_Investigatory_Powers_Act_2000
The Contempt of Court Act 1981	https://en.wikipedia.org/wiki/Contempt_of_Court_Act_1981
Copyright, Designs and Patents Act 1988	https://en.wikipedia.org/wiki/Copyright,_Designs_and_Patents_Act_1988
The Criminal Justice Act 1988	https://en.wikipedia.org/wiki/Criminal_Justice_Act_1988
Defamation Act 1996	https://en.wikipedia.org/wiki/Defamation_Act_1996
Human Rights Act 1998	https://en.wikipedia.org/wiki/Human_Rights_Act_1998
Obscene Publications Act 1959/ 1964	https://en.wikipedia.org/wiki/Obscene_Publications_Act_1959
Public Order Act 1986	https://en.wikipedia.org/wiki/Public_Order_Act_1986
Civil Evidence Act 1995	https://en.wikipedia.org/wiki/Hearsay_in_English_law
Communications Act 2003	https://en.wikipedia.org/wiki/Communications_Act_2003
The Companies Act 2006	https://en.wikipedia.org/wiki/Companies_Act_2006

Criminal Justice and Immigration Act 2008	https://en.wikipedia.org/wiki/Criminal_Justice_and_Immigration_Act_2008
Police And Justice Act 2006	https://en.wikipedia.org/wiki/Police_and_Justice_Act_2006
The Privacy and Electronic Communications (EC Directive) Regulations 2003	https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_(EC_Directive)_Regulations_2003
The Terrorism Act 2006	https://en.wikipedia.org/wiki/Terrorism_Act_2006
Employment Agency Act 2003	https://en.wikipedia.org/wiki/Conduct_of_Employment_Agencies_and_Employment_Businesses_Regulations_2003
European Union Legislation: Directive 95/46/EC	https://en.wikipedia.org/wiki/Data_Protection_Directive
European Union Legislation: Directive 97/7/EC	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al32014
European Union Legislation: Directive 2002/58/EC	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24120
Data Protection Act 2018	http://www.legislation.gov.uk/ukpga/2018/12/contents
Sanctions and Anti-Money Laundering Act 2018	http://www.legislation.gov.uk/ukpga/2018/13/contents
European Union (Withdrawal) Act 2018	http://www.legislation.gov.uk/ukpga/2018/16/contents

4.2 Understanding the needs and expectation of interested parties

Interested Parties	Information Requirements
Directors	• Ensure that the business continues to function in a profitable manner without hindrance and bureaucracy. • Ensure client satisfaction to retain current business and identify new business trends to pursue new clients • Ensure employees are delivering good quality in a safe and satisfactory environment
Employees	• Ensure good quality deliver in respect of company policies and standards • Meet and succeed clients' expectation • Report issues and concerns to management
Contractors	n/a
Suppliers	• Supply goods and services as required in respect of law compliance and company standards and requirements
Accountants	• Comply with financial and tax regulations • Monitor the accounts and inform Management about clients' insolvency
Company Solicitors / Lawyers	• Operate in the company's best interest when required to advise or act on the company's behalf
Governing Bodies	• Operate in respect of law compliance
Regulatory Bodies	• Operate in respect of rules and standards agreed between the company and the regulatory bodies
Unions	n/a
Shareholders	n/a

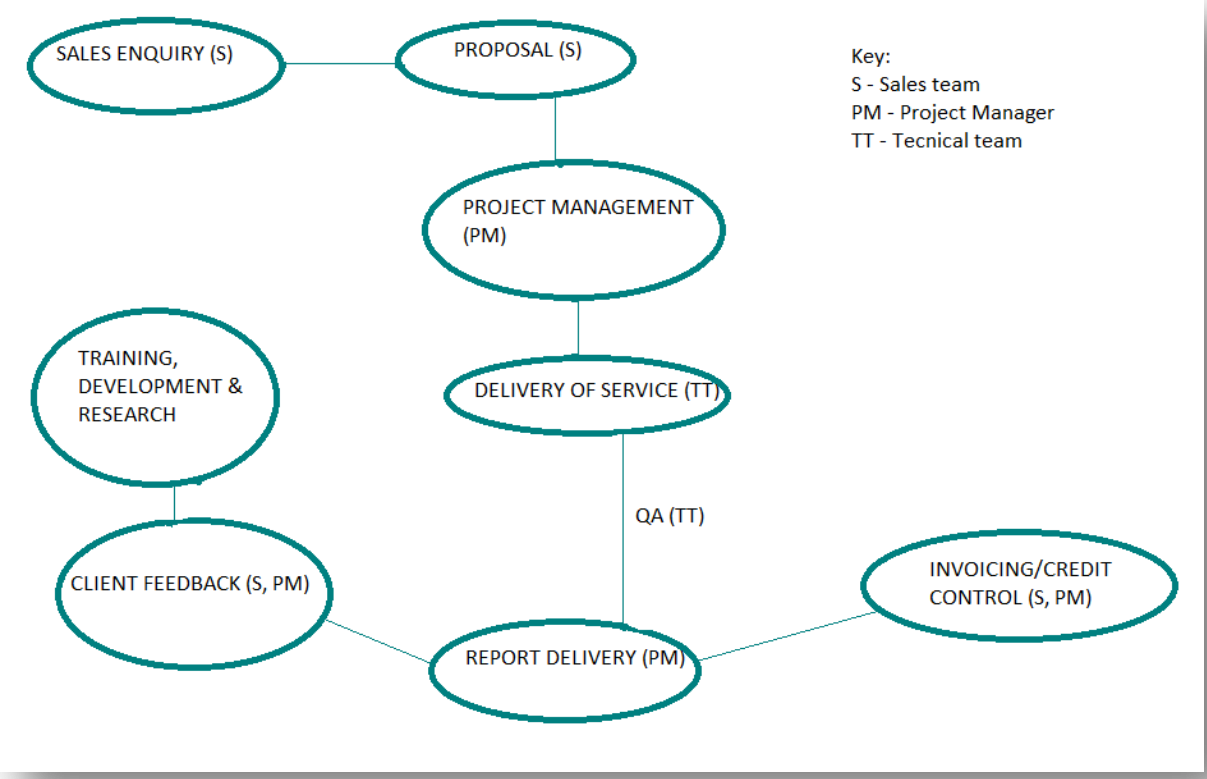
4.3 Determining the scope of the business management system which includes ISO 9001:2015 & ISO 27001:2013

Quality and Information Security

The scope of this policy relates to use of the assets and computer systems operated by the company at its office in London, in pursuit of the company's business of providing security consultancy services to its clients and achieve the Quality and Information Security objectives as described in 3. Objectives above.

4.4 Business Management system and its processes

SECFORCE is responsible for the planning and delivery of its services and ensuring that all information is held securely. We work closely with our partner suppliers and customers to satisfy mutual requirements. We have a flow chart of illustrate the interaction of our core business processes, as shown below:



A SWOT analysys of our realisation process is described in a stand alone document.

5 LEADERSHIP

5.1 Leadership & Commitment

SECFORCE's Top Management Team are committed to the development and implementation of a Quality & ISMS Policy and the Business Management System which are both compatible with the strategic direction and the context of the organisation, the whole system is frequently reviewed to ensure conformance to both ISO 9001:2015 and ISO 27001:2013 standards. Responsibility has been assigned to ensure that the business Management System conforms to the requirements of the respective standard and the provision to report on performance to the top management team has been defined.

The designated Senior Management Representative(s) will ensure that **SECFORCE** staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving **SECFORCE's** Quality & Information Security Policy and Objectives which are aligned with the organisations strategic direction

The Senior Management Team is responsible for implementing the BMS and ensuring the system is understood and complied with at all levels of the organisation.

In summary, the Senior Management Team will ensure that:

5.1.1 Leadership and commitment for the Business Management System

- The company has a designated Senior Management Representative who is responsible for the maintenance and review of the Quality Management Systems.
- The ongoing activities of **SECFORCE** are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process.
- Measurement of our performance against our declared Quality and Information Security Objectives is undertaken.
- Resources needed for the BMS are available and employees have the necessary training, skills and equipment to effectively carry out their work.
- Internal audits are conducted regularly to review progress and assist in the improvement of processes and procedures.
- Objectives are reviewed and, if necessary amended, at regular Management Review meetings and the performance communicated to all staff.
- The information security policy and objectives are established in line with the strategic direction of the organisation and that intended outcome(s) are achieved.
- The BMS is integrated into the organisations business processes.
- Communication covering the importance of the effective BMS and conformance to the BMS requirements is in place.
- Continual improvement is promoted.
- The contribution of persons involved in the effectiveness of the BMS is achieved by engaging, directing and supporting persons and other management roles within their area of responsibility.

5.1.2 Customer Focus

- Customer requirements and applicable statutory and regulatory reuirements are determined and met
- The risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed

- The focus on consistently providing products and services that meet customer and applicable statutory and regulatory requirements is maintained
- The focus on enhancing customer satisaction is maintained

5.2 Quality & ISMS Policy

The Quality & ISMS Policy of **SECFORCE** is located within section 1.3 of this Manual – Quality & ISMS Policy.

5.3 Organisational roles, responsibilities and authorities

SECFORCE has an organisation chart in place (See Organisation chart v1.2), employee contracts together with job descriptions to ensure that the appropriate personnel are in place to cover the whole context of the organisation and strategy of the business.

Our Information Security Manager (this role is carried out by Rodrigo Marcos) is responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

6 Planning for the Business Management System

6.1 Actions to address operational risk and opportunities

We have identified the business process as a means of identifying and determining the risks and opportunities that are relevant to our Business Management system; from an operational perspective a Risk & Opportunities analysis has been conducted as part of our SWOT analysis, separate to this manual.

Within each of the areas the risks (if any) are identified together with a rating as to the importance of the risk.

We use an Excel spreadsheet to collect and analyse the risks and opportunities for both Quality and Information Security.

The risk and opportunities document is reviewed annually by the Senior Management Team to ensure the effectiveness of the actions have been fulfilled.

The approach to our risk treatment plan (Statement of Applicability) has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – control objectives and controls) as a guide to establish that all controls required have been considered and that there are no emissions.

The document identifies controls to mitigate risks following the process of identification, analysis and evaluation described and is directly linked to the aspects of the organisation. The SOA document is separate to this Manual.

6.1.2 Information Security Risk Assessment

In accordance with 8.2 of the ISO 27001:2013 standard, we use an Excel spreadsheet to collect and analyse the risks identified in the following assets / asset groups:

- Buildings, offices
- People and reputation
- IT
- Critical third party suppliers
- Client information and data

All typical / likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) using a ratings scale of;

Very Low - 1, Low – 2, Medium – 3, High 4 and Very high – 5 and expressed across key areas of Vulnerability, Probability and Impact

Following this analysis, evaluations are drawn as to what the most appropriate action is together with the estimated cost of implementing action to address the identified issue and an estimate of the cost of ignoring the risk.

Key evaluation criteria use is 1 – Accept risk, 2 - Apply controls, 3 - Avoid risk, 4 – Transfer the risk.

6.1.3 Information Security Risk Treatment

The approach to our risk treatment plan has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – Control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions.

The document identifies controls to mitigate risks following the process of identification, analysis and evaluation described in section 7 and is directly linked to the aspects of the organisation.

The SOA document is separate to this Manual and conforms to the requirements as defined within clause 8.3 of the ISO 27001:2013 standard.

Please see below document as demonstration:-
SOA - Risk Assessments

6.2 Quality and ISMS Objectives and planning to achieve them

The Quality and ISMS Objectives and methods of achieving the objectives is located within section 3 of this Manual – Quality and ISMS Objectives.

6.3 Planning of Changes (QMS Only)

The Senior Management Team of **SECFORCE** identify any potential changes, this is then delegated to a responsible person as a "project manager".

He or she will conduct a "research background" to determine the feasibility of the changes with regards to:-

- Purpose of the change
- Any potential consequences
- Integration of the quality management system
- The availability of resources
- The allocation or reallocation of responsibilities and authorities
- Technical Skills
- Timescales
- Risks
- Impact

Once completed this then forms part of the Management Review together with including within the internal audit schedule.

Please see below document as demonstration:-
Planning of Changes

7 Support

7.1 Resources

7.1.1 General

SECFORCE determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the business management system.

We ensure that the below elements are taken into account when completing an evaluation:

- The capabilities of, and constraints on, existing internal resources;
- What needs to be obtained from external providers

7.1.2 People

Operation and context of the organisation is taken into account when we determine the relevant persons necessary for the effective operation of the business management system.

7.1.3 Infrastructure

All of our administration is conducted at our Head Office. This includes:-

- Management of financial matters
- Handling of client orders
- Personnel records

In terms of equipment used to deliver our services, asset registers and maintenance records are kept for the following:

- Infrastructure
- Web services

7.1.4 Environment for the operation of processes

The main environment consists of an open space area which can accommodate up to 13 people. Heating is provided by the building management and controlled manually. Chairs are adjustable and staff are equipped with a laptop stand and hydraulic monitor arm upon request. There are no psychological factors to take into consideration. The ergonomic layout is good minimising any impacts to the environment.

7.1.5 Monitoring and measuring resources

We ensure that all relevant equipment and personnel are monitored and measured to ensure that equipment and personnel are effective for the services we offer:-

Equipment: We ensure that all equipment is serviced, maintained and where applicable calibrated to statutory and regulatory requirements. PAT tests and maintenance of fire extinguishers are conducted regularly

Personnel: We ensure that all personnel are monitored on a regular basis. (We maintain a checklist for joiners and leavers as evidence. Yearly meetings are held between each member of staff and senior management.

7.1.6 Organisation Knowledge

We ensure that "Job Specifications" are produced which include knowledge requirements for each individual role. Specific tests are implemented to ensure that persons are knowledgeable with the specific elements of the role. This could include telephone interview, tests, internal training or vocational certificates.

7.2 Competence

All employees have the training and skills needed to meet their job requirements. All employees are monitored on an ongoing basis to identify any training and development needs. Competences and training needs are identified / satisfied by using:

- Job descriptions which set out the competences required
- Contracts of employment which set out contractual and legal requirements
- Induction starter pack
- Verbal appraisal reviews
- Development plans to set objectives
- A practical training course upon employment

7.3 Awareness

We ensure that all employees are aware of all policies and their contribution to the effectiveness of the Business Management System through:

- Induction starter pack
- SECFORCE wiki

7.4 Communication

For internal staff the company wiki is a source of information and is updated regularly to ensure that all information is correct. This is accessible by all staff.
Any communication which is sent external to the wiki is designated through the appropriate line manager.

For external persons, information on company policies and processes are provided upon request.

7.5 Documented Information

7.5.1 General

SECFORCE demonstrates documented compliance to ISO 9001:2015 through this Business Management System Manual (which includes processes & procedures) on an electronic system which is available on the company wiki. All information is read only and only accessible via the document owner for amendment.

7.5.2 Creating and updating

The creation of documentation to support the Business Management System is primarily the responsibility of the designated "Top Management Representative".

Identification will be sought by a document number, date and author. To aid the approval and suitability of documents, the Managing Director of **SECFORCE** authorises the release and delegates any training required to the "Top Management Team".

7.5.3 Control of documented information

All documentation is controlled by version and date.

Generic documents can be retrieved by authorised personnel from \\172.16.16.160\operations.
Customer records are identified by customer name and project ID and stored in \\172.16.16.160\projects .
Other documentation for internal use only is listed in Master Document List.doc 7 - Support\Master Document List v1.1.docx)

On or after the retention period stated, the relevant records will be reviewed by Top Management and will either remain in-situ, be archived or destroyed.

If records are to be destroyed, they will be disposed of in a controlled manner; *sensitive hard copies will be shredded and soft copies will be deleted from the system*. If records are to be archived, they will be identified and stored appropriately

8 Operation

8.1 Operational planning and control

SECFORCE has determined the requirements and controls implemented for all processes detailed in section 4.4. Any planned changes are controlled through section 6.3 (Planning for Changes)

8.2 Determination of requirements for products and services

8.2.1 Customer Communication

Capability, facility and service information is supplied to customers via web site, brochures, email and through direct sales / personal contact.

Communications such as quotes, orders and amendment details are appropriately stored and identified by customer and project ID.

Customer feedback is proactively sought via direct contact and satisfaction monitoring.

Complaints are documented and recorded on the SECFORCE Scheduler Administration tool (http://172.16.16.161:82/admin/feedback/feedback).

8.2.2 Determination of requirements related to products and services

SECFORCE ensures that applicable statutory and regulatory requirements are met which can be evidenced within section 4.1 of this document.
Should we issue any legal documentation (i.e. calibration document – traced back to national standards) in connection with the services offered then this is forwarded to the clients at the closure of the contract. All documentation is filed within the client file for archive purposes.

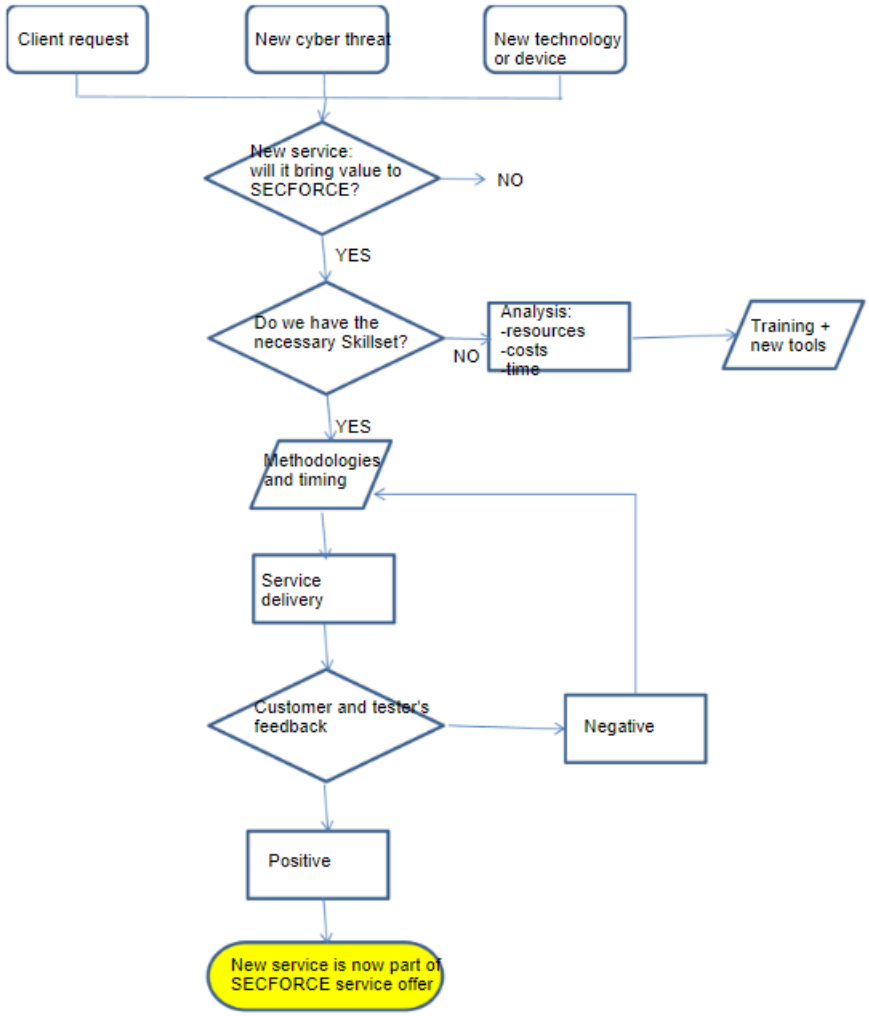
8.2.3 Review of requirements related to products and services

SECFORCE has processes in place to ensure that client details are collected at the closure of the contract. This to ensure that all details are correct and any additional information is collected etc.

Any change required either through client requirements or service design will be fully documented through the "Planning of changes" within section 6.1 of this document.

8.3 Design and development of products and services

SECFORCE has detailed processes for the design and development of services.



8.3.2 Design and development planning

The initial stage of **SECFORCE** design and development process begins with the varius reason why there might be an appetite for a new type of service. Top Management discuss whether the new service would bring value to the company, ex. Can the new service be integrated in our current service offer and be sold to a number of clients? Another major point is to understand if we currently have the right skill and toolset. If we don't, an analysis will be conducted on costs and time necessary to acquire the new skills and purchase the new tools.

8.3.3 Design and development inputs

If Top Management agrees that the costs to implement the new service will be covered by selling such service, the technical team is provided with training and new equipment/tools.
When a satisfactory competence is achieved, methodologies are prepared and an estimate time effort per task is established.

8.3.4 Design and development controls

The service delivery is firstly simulated in house, then offered to the client.
If the client provides a negative feedback, ex. the results are not compliant with the expectations, the service methodologies are re-examined. The same happens if the tester provides a negative feedback on his own service delivery, ex. the training provided was not sufficient or an unexpected issue arose.

8.3.5 Design and development outputs

If both client and tester's feedback are positive, the service is formally included within Secforce service offer and its quality is continuously monitored through customer feedback.

8.3.6 Design and development changes

Customer feedback is regularly reviewed and, when needed, the service delivery is amended to meet clients' needs.

8.4 Control of externally provided products and services

8.4.1 General

SECFORCE ensures that externally provided processes, products and services conform to specified requirements.

8.4.2 Type and extent of control of external provision

SECFORCE have controls in place to ensure that new external provisions are approved before using the service or product. This is initially done by checking the company public records on https://beta.companieshouse.gov.uk/.
Reputation and online reviews are also taken into consideration.
Regular suppliers (ex. utilities, drinking water) also undergo a price compare.
Once the supplier is engaged, the quality of service is reviewed yearly based on the following KPIs:

1. Performance: efficiency and delivery of contractually agreed services
2. Incidents: events that have negatively impacted our business
3. Billing: accuracy and timeliness of billing, order processing, prices, etc
4. Quality: supplier responsiveness, customer service, supplier knowledge, etc

Local suppliers/SME whose reputation can't be verified online are also checked via the Supplier Quality Questionnaire, to be sent on a yearly basis.

Please see below document(s) as demonstration of compliance:
Supplier Quality Questionnaire
Approved Suppliers List

8.4.3 Information for external provision

Communication of any applicable requirements which are deemed appropriate and are provided through the contract review with the provider. (i.e. T&C's, performance, competence etc)

8.5 Production and service provision

8.5.1 Control of production and service provision

SECFORCE ensures that controls are in place for conditions for production and service provision, including delivery and post-delivery activities.

8.5.2 Identification and traceability

Projects are scoped based on to the client requirements and a typology of test is identified accordingly, to each of which corresponds a specific methodology. When quotes are accepted by the client, a sales order is created to inform the project management team about client's requests and timelines.

8.5.3 Property belonging to customers or external providers

SEFCORCE never pertain customer properties. If a specific device is sent to the office for testing, arrangements are in place for the customer to retrieve it upon project completion.

8.5.4 Preservation

Devices specified above are kept locked until project completion, when are then packed safely to ensure no damage is caused.

8.5.5 Post-delivery activities

Upon report delivery, SECFORCE state its availability to assist and provide clarifications. Retests are also offered to verify whether remediation of the vulnerabilities originally discovered have been completed and implemented correctly.

8.6 Release of products and services

SECFORCE ensures that the appropriate documentation is provided to the client on release of the service and this is also retained for traceability.
eg. Final reports, certificates, letters of compliance, spreadsheets of findings, encrypted emails.

8.7 Control of nonconforming process outputs, products and services

The **SECFORCE** Scheduler Administration tool, Feedback section, is used to identify non-conformances and any actual or potential shortfalls in quality standards or internal processes/ procedures, suggest improvements and track any actions to ensure improvements have taken place, or potential problems are avoided.

These areas are reviewed within the agenda for the Management Review meetings and typically cover the action taken to control and correct any non conformances noting any consequences of the action taken and themes which may be evident. In terms of continual improvement, we also review the suitability, adequacy and effectiveness of our Business Management System.

SECFORCE has various processes and procedures in place to ensure that preventative action against nonconformities can be introduced, documented and seen through to completion in order to address the initial problem. The complex nature of the clients we work with demands that we have flexible, but effective, processes and procedures in place.

However, SECFORCE also uses internal and external audits and risk assessments to continuously improve its service delivery, financial, HR and operational functions.

Steps

- The Management Representative maintains and monitors the feedback log on the SECFORCE Scheduling Administration tool.
- If any person discovers a shortfall, or potential shortfall in the written processes/procedures or a problem in the practical application of them, the details must be documented in the SECFORCE Scheduling Administration tool. The relevant person who is responsible for the action is informed. Action required as a result of Customer Feedback, Customer Complaint, Information Security incident or Management Review is also logged and tracked via the SECFORCE Scheduling Administration tool.
- Each entry in the Action Log to include:
    a. Date recorded
    b. Overview of the issue, problem or concern
    c. Person/team responsible
    d. Action taken
    e. Date completed

9 Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

Monitoring is based on Risk and is linked to the SWOT analysis of processes together with the risk assessments which are carried out yearly.

9.1.1 General

SECFORCE has deemed the following elements (9.1.2 & 9.2) for monitoring, measuring, analysis & evaluation to ensure the quality performance and the effectiveness of the business management system.

9.1.2 Customer Satisfaction

SECFORCE collates data on customer satisfaction through various means. This includes customer contact, emails and customer spontaneous feedback.

9.1.3 Analysis and Evaluation

Results of feedback which includes customer feedback, conformity of services, planning, risk & opportunities matrix (see SWOT) is evaluated through the management review meeting and actioned as applicable should any non-conforming areas be present.

9.2 Internal Audit

An internal audit schedule is prepared on an annual basis year and covers the requirements of any ISO standards against which **SECFORCE** will be assessed. Internal audits are carried out through "risk or clause based" auditing.

Appropriate personnel are allocated to complete the internal audits and must record appropriate evidence for completeness. All audits completed must be authorised by Top Management as complete once any non-conforming areas have been dealt with (without any undue delay). Internal audit documentation must be kept and filed appropriately.

9.3 Management Review

Management reviews take place on a bi-yearly basis. The attendees present are "Top Management" and any other appropriate persons of the business.

All inputs / outputs are documented in line with the requirements of the specific ISO standard against which **SECFORCE** will be assessed. Any actions arising from the meeting must be completed without any undue delay and appropriate evidence filed with the Management review documentation.

10 Improvement

10.1 General

SECFORCE ensures that improvement processes are completed and actioned as necessary. Analysis methods include various elements which include:-

- Customer feeback
- Planning changes to the Quality Management System & Services
- 3rd party assessments for certification purposes
- Risks & Opportunities

10.2 Nonconformity and corrective action

Should a nonconformity occur, including those arising from complaints, internal audits & external 3rd part assessment **SECFORCE** designate the appropriate "Top Management" representative to ensure that corrective action including root cause analysis is completed and implemented to avoid any further occurrences. This is then analysed and should the risk to the business pose to be "high" then this is then entered onto the Corrective Action Form to assist in mitigating the risk to the business.

The corrective action plan summary must be completed, as this then forms part of the Management Review meeting.

Please see below document(s) as demonstration of compliance:
Previous year summary report
Corrective Action Plan

10.3 Continual Improvement

Continual Improvement will be ongoing through various elements of the Business Management System which is encompassed within this document. The list below is not exhaustive:-

- Risk & Opportunities Analysis – Evaluated at several stages (clause 5.1, 6.1)
- Quality Policy / Objectives
- Planning of Changes
- Competency Matrix
- Customer Satisfaction
- 3rd Party External Audits
- Management Review