

The BS7799 Security Standard

The British Standard 7799, BS7799, is the most widely recognised security standard in the world. The last major publication was in May 1999, an edition which included many enhancements and improvements on previous versions. In December 2000 it was republished again, and evolved into ISO17799

BS7799 (ISO17799) is comprehensive in its coverage of security issues. It contains a significant number of control requirements, some extremely complex. Compliance with BS7799 is consequently a far from trivial task, even for the most security conscious of organizations. Full certification can be even more daunting.

It is therefore recommended that BS7799 is approached in a 'step by step' manner. The best starting point is usually an assessment of the current position/situation, followed by identification of what changes are needed for BS7799 compliance. From here, planning and implementing must be rigidly undertaken.

This web site is intended to assist with this process. It will provide further information on the BS7799 standard, as well as suggesting a solution to help guide you to full compliance.



[What is BS7799?](#)

[How is it Organized?](#)

A description of BS7799 and very good starting point for the unfamiliar.



[Compliance Strategy](#)

How to approach the BS7799 issue from a compliance perspective.



A Recognised and Proven Solution

Details of the acclaimed COBRA methodology and tool (including a downloadable trial copy).



The Risk Dimension

Risk analysis is a fundamental requirement for compliance with BS7799.



BS7799 and Security Policies

A leading source for comprehensive and BS7799 compliant information security policies.

The BS7799 Security Standard: What is It?

BS7799 is a very detailed security standard. It is organized into ten major sections, each covering a different topic or area:

1. Business Continuity Planning

The objectives of this section are as follows: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control

The objectives of this section are as follows: 1) To control access to information 2) To prevent unauthorised access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect unauthorised activities. 6) To ensure information security when using mobile computing and tele-networking facilities



3. System Development and Maintenance

The objectives of this section are as follows: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data.

4. Physical and Environmental Security

The objectives of this section are as follows: To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

5. Compliance

The objectives of this section are as follows: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the

effectiveness of and to minimize interference to/from the system audit process.

Within each section are the detailed statements that comprise the standard.

The BS7799 Security Standard: A Strategy for Compliance

Before considering full certification, or indeed any formal public statement on the BS7799 issue, it is essential to gain confidence in your underlying compliance level. Essentially, establishing your current compliance position is the first step to conformance with the standard.

This is actually much harder to achieve than may superficially appear. For larger organizations, the position of each and every information system within scope needs to be established. This CAN be a very intensive and costly operation indeed.

Having achieved this, plans now need to be created to ensure that the identified improvements and changes are implemented. This again CAN prove to be very costly.

However, having completed this process, and having reached a broad but deomstrable compliance plateau, most of the hard work is actually done.

The [next page](#) will consider a method of simplifying the above and achieving full compliance with minimum pain.

A Recognised BS7799 Audit and Compliance Solution

Achieving compliance with BS7799 is a substantial task. Assessing compliance levels for information systems, and then creating/implementing the necessary plans to become fully compliant, can be a very intensive process indeed. However, with the correct approach and method this effort can be minimized.

Probably the most efficient and cost effective method of achieving this is via the use of a software product. This ensures consistency as well as bringing a degree of automation to the exercise. **COBRA BS7799 Consultant** was designed specifically to make BS7799 compliance far easier and much more straight forward.

The **COBRA** product guides you through the entire audit/compliance exercise. Through each of the ten sections, via a series of online questions, **COBRA** will take you through the whole standard. It then creates comprehensive reports to:

- Explain your current BS7799 compliance position with respect to each of the ten sections
- Identify what your shortcomings and failings are
- Give detailed recommendations on exactly what steps are necessary to rectify these problems and thus achieve compliance.

Basically, it will objectively assess your position with respect to BS7799, generating both guidance and specific recommendations. It offers a unique and distinct approach to BS7799 compliance... one which we believe will prove invaluable to all types and sizes of organization.

DOWNLOAD A TRIAL COPY

The best way to establish whether it is suitable for you is to "try before you buy". For a fully function evaluation copy, visit the COBRA [*download](#)

page*.

A Recognised BS7799 Audit and Compliance Solution

Achieving compliance with BS7799 is a substantial task. Assessing compliance levels for information systems, and then creating/implementing the necessary plans to become fully compliant, can be a very intensive process indeed. However, with the correct approach and method this effort can be minimized.

Probably the most efficient and cost effective method of achieving this is via the use of a software product. This ensures consistency as well as bringing a degree of automation to the exercise. **COBRA BS7799 Consultant** was designed specifically to make BS7799 compliance far easier and much more straight forward.

The **COBRA** product guides you through the entire audit/compliance exercise. Through each of the ten sections, via a series of online questions, **COBRA** will take you through the whole standard. It then creates comprehensive reports to:

- Explain your current BS7799 compliance position with respect to each of the ten sections
- Identify what your shortcomings and failings are
- Give detailed recommendations on exactly what steps are necessary to rectify these problems and thus achieve compliance.

Basically, it will objectively assess your position with respect to BS7799, generating both guidance and specific recommendations. It offers a unique and distinct approach to BS7799 compliance... one which we believe will prove invaluable to all types and sizes of organization.

DOWNLOAD A TRIAL COPY

The best way to establish whether it is suitable for you is to "try before you buy". For a fully function evaluation copy, visit the COBRA [*download](#)

page*.

Introduction to Security Risk Analysis

Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.

However, many conventional methods for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility, and critically... in terms of what they produce for the user.

This site is intended to explore the basic elements of risk, and to introduce a security risk assessment methodology and tool which is now used by many of the worlds major corporations. It also embraces the use of the same product to help ensure compliance with security policies, external standards (such as ISO 17799) and with legislation (such as Data Protection legislation).

The following topics are covered:

- [Introduction To Security Risk Analysis and Risk Assessment](#)
- [Introduction To The COBRA Approach](#)
- [COBRA Risk Consultant Features](#)
- [The COBRA Security Risk Assessment Process](#)
- [COBRA Module Manager](#)
- [COBRA Risk Assessment & Security Risk Analysis Knowledge Bases](#)
- [Other COBRA Products](#)

Having reviewed these pages, you may wish to [purchase the COBRA product](#) or perhaps [** download the software **](#) for trial/evaluation.

Alternatively, if you have any questions on any aspect of this approach to risk analysis and security risk assessment, please do not hesitate to [contact us](#).

Introduction to Risk Analysis

Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective, is quite often a complex and sometimes a subjective matter. One of the prime functions of security risk analysis is to put this process onto a more objective basis.

There are a number of distinct approaches to risk analysis. However, these essentially break down into two types: quantitative and qualitative.

Quantitative Risk Analysis

This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.

Quantitative risk analysis makes use of a single figure produced from these elements. This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability.

It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.

The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.

Notwithstanding the drawbacks, a number of organisations have successfully adopted quantitative risk analysis.

Qualitative Risk Analysis

This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used.

Most qualitative risk analysis methodologies make use of a number of interrelated elements:

THREATS

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.

VULNERABILITIES

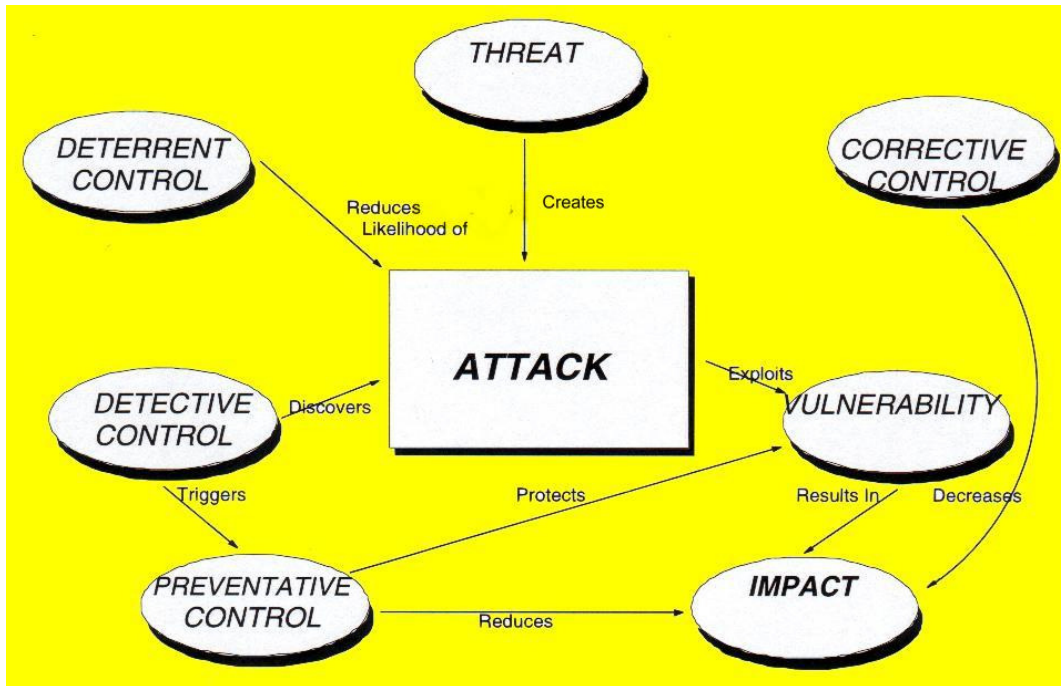
These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire a vulnerability would be the presence of inflammable materials (e.g. paper).

CONTROLS

These are the countermeasures for vulnerabilities. There are four types:

- Deterrent controls reduce the likelihood of a deliberate attack
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model:



The knowledge base supplied with **COBRA Risk Consultant** employs this methodology and variations of it.

Introduction to COBRA

COBRA, or 'Consultative, Objective and Bi-functional Risk Analysis', consists of a range of risk analysis, consultative and security review tools. These were developed largely in recognition of the changing nature of IT and security, and the demands placed by business upon these areas.

The first such undercurrent of change was the growing acceptance that IT security was a business issue. It was, and is, becoming largely expected that security reviews should be business related, with cost justified solutions and recommendations.

Another issue, very much of the late 90s, is the search by many organisations for a better and more visible return on their security budgets. To achieve this many

adopt new approaches to the traditional constraints of lack of expertise, time and finance.

Often, a formal risk analysis technique is employed. However, conventional methods and tools simply do not address the new demands placed by business management. Some go part of the way, but tend to introduce their own drawbacks and difficulties.

COBRA, and its default methodology, evolved very much to tackle these issues properly. It was developed in full co-operation with one of the world's major financial institutions and followed many years of research.

It was recognised that business users should be involved from the outset. This carries a number of advantages, and shapes the entire review. In addition, a number of other radical departures were called for.

The result was a risk analysis methodology and tool that will meet the most stringent of requirements, fully satisfying the changing demands placed upon the security or audit team.

This site will outline the main features of **COBRA**, as well as providing some background into security risk analysis itself.

COBRA Risk Consultant

Features

COBRA Risk Consultant provides a complete risk analysis service, compatible with most recognised methodologies (qualitative and quantitative). It is a questionnaire based PC system using 'expert' system principles and an extensive knowledge base.

It evaluates the relative importance of all threats and vulnerabilities and generates appropriate recommendations and solutions. In addition, its reports provide a written assessment and relative risk score, or level, for each risk category. The risks identified are automatically linked with the potential implications (financial, customer loss, etc.) for the business or department.

Flexibility

A major feature is the modularisation of the **Risk Consultant** knowledge base. This enables question modules to be directed at personnel with the appropriate expertise and knowledge. For new developments, it also allows a stage by stage assessment (design, development, acceptance testing & implementation). As well as increasing accuracy, this approach enables more detail and precision and thus ensures better results and solutions.

Automatic Customisation

No two enterprises are the same, and neither are their security requirements. **Risk Consultant** will therefore generate questionnaires, from 'knowledge base' question modules, that are specifically suited to the organisation, environment and system under evaluation. This function is also performed dynamically as questions are answered and **Risk Consultant** obtains more information.

Self-Analysis

COBRA Risk Consultant is designed to be truly self-analytical. It can be used without the need for detailed security knowledge or expertise in using risk management software. There is no need to hire expensive consultants to back-up the system.

Solution Testing

'Hypothesis testing' is fully supported. The impact that specific additional controls would have on a system's risk level can be dynamically ascertained. It is thus possible to quickly establish the most cost effective solution to individual exposures.

Reports

The reports produced by **Risk Consultant** are NOT standard computer output. They are professional business reports and are suitable for interpretation by both technical and non-technical management.

A range of report formats are available, and for maximum flexibility all sections are optional. In addition, output can be directed to paper, to a terminal, or to a file (for possible import into a word processing package).

The Risk Assessment Process

The risk assessment process, using COBRA, is extremely flexible. A substantial number of approaches are supported. However, the default process usually consists of three stages:

- [Questionnaire Building](#)
- [Risk Surveying](#)
- [Report Generation](#)

During the first stage, via module selection or generation, the base questionnaire is built to fit the environment and requirements of the user.

The second stage is the survey process - **Risk Consultant** questions are answered by appropriate personnel and the information is securely stored.

For the third stage risk assessments and 'scores' are produced for individual risk categories, individual recommendations are made and solutions offered, and potential business implications are explained.

Each of these stages is managed by its corresponding system component: **Questionnaire Builder, Risk Surveyor or Report Generator.**

Questionnaire Builder

Questionnaire Builder constructs an appropriate risk questionnaire for the environment/system under consideration. Individual 'Question Modules' are specifically selected from the knowledge base.

Each module embraces a particular area of risk or a specific threat class (e.g. Logical Access, Physical Access, Networks, Development, Operations, etc).

The questionnaire building process can be performed either manually or automatically:

Automatic Questionnaire Building

With an automatic questionnaire build, the system creates a questionnaire that suits the user's system/installation specifically. This is achieved through completion of the initial 'Business' or 'Impact' Questionnaire.

Configuration, business function(s) and many other factors are taken into consideration, as well as the financial significance of each area of the system and its potential for loss (direct or indirect). The business user can, therefore, be involved from the outset.

The Business (or Impact) Questionnaire covers each category in turn and upon completion generates a 'significance level' for each. This 'significance level' determines which question modules *Questionnaire Builder* will select for inclusion in the detailed questionnaire.

Manual Questionnaire Building

A manual questionnaire build may be desirable for a variety of reasons:

- consideration of a specific aspect of security/risk
- performing risk analysis in various proposed scenarios
- analysis of all risk areas, even if some are not of real significance to the organisation.

The questionnaire is created by user selection of individual question module(s) from those defined to ***Risk Consultant***.

Dynamic Building

Although the questionnaire is thus constructed, the user can return to the *Questionnaire Builder* at any stage to add or remove question modules.

Risk Surveyor

Risk Surveyor manages the questionnaire completion process. The question modules which comprise the questionnaire are completed individually, each by appropriate personnel.

Different modules can also be completed at different times, enabling scheduling to be based around personnel availability. The results are brought together at the report generation stage.

The Question Modules

Questions are of various formats; mandatory single response, optional single response, mandatory multiple response, optional multiple response, text response, and numeric response. Most are of a simple, multiple choice variety.

Full branching facilities are included, including the facility to branch to a secondary question module and return to the original. All input is validated and screens are of a standard format.

The ability to skip one or more questions (for later completion) is also provided, along with a 'notepad' facility to enable additional comments and notes to be recorded. In addition, further question modules may be dynamically generated as questions are answered and **Risk Consultant** obtains more information.

A comprehensive help facility is provided at both system and question level.

Report Generator

The *Report Generator* is used to produce the results from the completed questionnaire. The results are suitable for interpretation by both technical and non-technical management and are in the form of a professional business document.

Report Content

A number of report sections are provided:

- Recommended solutions and specific additional security control suggestions
- A descriptive assessment and relative risk score for each 'risk category' in each area considered
- A full impact analysis for the business or department
- Direct linkage between areas of risk and the potential financial and business implications.

Report headings and the introductory text for each section can be changed and tailored to reflect user requirements and culture.

Output Channels

Reports can be produced on the PC monitor or on a printer. Output can alternatively be directed to a file. This enables import to word processing packages, if required.

System Control

A wide range of system parameters are user definable, including screen colours, sub-folders, etc.

Introduction to Security Risk Analysis

Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.

However, many conventional methods for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility, and critically... in terms of what they produce for the user.

This site is intended to explore the basic elements of risk, and to introduce a security risk assessment methodology and tool which is now used by many of the worlds major corporations. It also embraces the use of the same product to help ensure compliance with security policies, external standards (such as ISO 17799) and with legislation (such as Data Protection legislation).

The following topics are covered:

- [Introduction To Security Risk Analysis and Risk Assessment](#)
- [Introduction To The COBRA Approach](#)
- [COBRA Risk Consultant Features](#)
- [The COBRA Security Risk Assessment Process](#)
- [COBRA Module Manager](#)
- [COBRA Risk Assessment & Security Risk Analysis Knowledge Bases](#)
- [Other COBRA Products](#)

Having reviewed these pages, you may wish to [purchase the COBRA product](#) or perhaps [** download the software **](#) for trial/evaluation.

Alternatively, if you have any questions on any aspect of this approach to risk analysis and security risk assessment, please do not hesitate to [contact us](#).