



# White Paper: Bsafe/Enterprise Security and ISO 17799

## What's it all about?

ISO 17799 is, arguably the most widely recognized security standard. It's all about information security and how to go about achieving it. It is a code of practice and detailed list of controls by which a reasonable level of information security can be attained in an organization. It lays out the process for establishing the security requirements of an organization, including risk assessment, the understanding of various legal and contractual requirements and the analysis of the organization's business objectives and processes.

The contribution that can be made by **Bsafe/Enterprise Security** is indicated already in the introductory pages of the standard. Here, various controls for information security are highlighted, such as data protection, safeguarding of records, information security policy, allocation of information security responsibilities and the reporting of security incidents.

The main chapters detailing the standard are:

4. Organizational Security
5. Asset Classification and Control
6. Personnel Security
7. Physical and Environmental Security
8. Communications and Operations Management
9. Access Control
10. Systems Development and Maintenance
11. Business Continuity and Management
12. Compliance

The scope is large, as can be understood from the chapter titles, and the kinds of activity discussed diverse, ranging from employee rules of behaviour to disaster recovery.

**Bsafe/Enterprise Security** is positioned to cover many of the issues discussed. Following is a detailed table giving the relevant issue, its place in the ISO 17799 standard and exactly how Bsafe/Enterprise Security answers the demand.



## Mapping of Bsafe/Enterprise Security Features to ISO 17799

### The ISO Paragraph

### The Specific Bsafe/Enterprise Security functions to Facilitate the Requirement

#### 4 Organizational Security

##### 4.1.3 Allocation of information security responsibilities.

Includes definition and documentation of authorization levels

1. Role Manager. Allows you to define different levels of administrator access to different users.

##### 4.2.1 Identification of risks from third party access.

Covers the types of access given to an organization's databases and information systems, types of third parties – staff, partners etc.

1. Application Access Control. Prevents unauthorised network access.
2. IP address manager. Defines ranges of permitted IP addresses for network access.
3. Application Audit. Monitors access and shows details of accesses made to the iSeries through the network.

#### 6 Personnel security

##### 6.3 Responding to security incidents and malfunctions.

Minimization of damage from security breaches through monitoring and learning

1. Application Audit. Monitors access and shows details of accesses made to the iSeries through the network.
2. IDS. Intrusion detection system to send instant alerts following unauthorized access attempts.
3. Application Analyzer. Graph-based tool to show trends in network access to the iSeries.

#### 8 Communications and operations management

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be passed on to any party, individual or organization without the express permission of Bsafe Information Systems. [www.bsafesolutions.com](http://www.bsafesolutions.com)



## The ISO Paragraph

## The Specific Bsafe/Enterprise Security functions to Facilitate the Requirement

### 8.3.1 Controls against malicious software.

Detection and prevention including control of system access

1. Application Audit with a particular emphasis on restrictions to the iSeries IFS (integrated file system)
2. IDS. Intrusion detection system to send instant alerts following unauthorized access attempts.

### 8.5.1 Network controls

Maintaining security in computer networks. Controls to safeguard the confidentiality and integrity of data passing over public networks and to protect the connected systems

1. Application Access Control. Limits access to individual internal servers (FTP, Telnet..)
2. File Audit to monitor changes at the file, record and field level.

## 9 Access Control

### 9.1.1 Access control policy

Control of access to information and business processes. Rules based on the premise "What must be generally forbidden unless expressly permitted".

1. Application Access Control. Enforces restrictions for all users through system defaults combined with permissions definitions for specified individuals or groups.
2. PC GUI. Easy to review and understand permissions definitions which have been made.

### 9.2.2 Privilege management

Restriction of powerful profiles which may access to important system resources

1. Application Access Control. Restricts all users to the definitions made in Bsafe/Enterprise Security without pre-defined rights. Even user QSECOFR is bound by the restrictions made.

### 9.2.4 Review of access rights

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be passed on to any party, individual or organization without the express permission of Bsafe Information Systems. [www.bsafesolutions.com](http://www.bsafesolutions.com)



## The ISO Paragraph

Check of privileges at regular intervals.

### 9.4

#### Network access control.

Controlling of access to both internal and external networks. Controls and procedures to protect networks and network services, segregation of networks and network connection control.

### 9.5

#### Operating system access control.

Identifying the ID of users, recording successful and failed system accesses, restricting connection times of users, automatic terminal identification, password management.

## The Specific Bsafe/Enterprise Security functions to Facilitate the Requirement

1. PC GUI based Object Authorization Manager, User Profile Manager and other functions make easy work of making and reviewing permissions definitions.
2. Authorization inquiry.
3. Password inquiry.

1. Application Access Control to restrict user access to service, function, library, object and IFS path.
2. Easy definition of port restrictions.
3. Control over multiple iSeries servers from a single PC client.
4. Access restriction by computer for DDM, pass-through and DRDA operations.
5. SSL encryption to assure the connection between Bsafe/Enterprise Security GUI client and iSeries server.

1. Secure Gateway (see above) to restrict user access to specific times and days.
2. Application Audit of network events.
3. Intuitive system journal display, filtering and management.
4. IDS to notify immediately of specified events including failed login attempts.
5. Automatic signon and device restrictions.
6. System value inquiry to quickly and easily review all system values through the GUI screen.
7. Password inquiry to easily identify password expiry dates and passwords identical to user IDs.
8. Easy GUI control of audit policy to



## The ISO Paragraph

## The Specific Bsafe/Enterprise Security functions to Facilitate the Requirement

make easier the task of defining the policy.

### 9.6 Application access control

Prevention of unauthorized access to information held in information systems, including access to groups of users. Information access restriction by control read, write, delete and execute functions.

1. Secure Gateway to restrict user access to specific server function, library, object and IFS path.
2. OS/400 object authority management by Bsafe/Enterprise Security GUI.
3. Restriction by user ID, generic name, group profile, Bsafe group (simply-managed, user-defined groups), IP address, system default.

### 9.7. Monitoring system access and use

Detection of unauthorized access, deviation from defined access policy, event logging and monitoring including user ID, date and time, type of events.

1. IDS to notify immediately of specified events including failed login attempts.
2. Application Audit of network events to examine access through the network.
3. Intuitive system journal display, filtering and management.
4. Application Analyzer – a set of graphs to display trends in network access to the iSeries.

### 9.8 Mobile computing and teleworking

Use of communications technology to enable staff to work remotely from a fixed location outside of the organization.

1. Secure Gateway to restrict user access to specific server function, library, object and IFS path.
2. IP address control for Telnet, including allowing only specified users to each IP address.
3. Time and day restrictions.