

# CORSAIRE

EXPERTS AT SECURING  
— INFORMATION —



## IT CHALLENGES FOR 2007 THE EMERGING STANDARDS: ISO27004 AND BS25999

<b>Document Reference</b>	The Emerging Standards: ISO27004 and BS25999 v2.0.doc
<b>Document Revision</b>	2.0
<b>Date</b>	05 June 2007



## Table of Contents

<b>TABLE OF CONTENTS.....</b>	<b>2</b>
<b>1. INTRODUCTION.....</b>	<b>3</b>
<b>2. SECURITY METRICS AND MEASUREMENTS .....</b>	<b>5</b>
2.1 What Metrics should be used? .....	6
2.2 IT Security Metric Example .....	7
2.3 What Metrics Do Not Tell You .....	9
2.4 Security Metrics Conclusion.....	9
<b>3. BS25999 BUSINESS CONTINUITY MANAGEMENT (BCM).....</b>	<b>11</b>
3.1 Implementing a BCM Solution .....	12
3.2 BS25999 Conclusion .....	16
<b>APPENDIX A.....</b>	<b>17</b>
References .....	17
Security Metrics and Measurements.....	17
BS25999.....	17
Acknowledgments .....	17
About the Author.....	17
About Corsaire .....	17



# The Emerging Standards: ISO27004 and BS25999

---

## 1. Introduction

IT systems and security, as business disciplines, continue to develop and mature. The importance to the financial well being of a company is now more fully appreciated (certainly within the realms of large corporations). This is reflected in the increasing number of senior management and board level appointments with responsibility for IT security.

The recognition has also been driven by the statutory requirements introduced by governments in the United States and the United Kingdom. Of particular interest to companies in the UK are the Computer Misuse Act, the Data Protection Act, the Companies Act and perhaps less well understood, the Regulation of Investigatory Powers Act.

An increase in IT security awareness is also reflected in the revised Data Protection Act, which now carries considerably more venom in the form of the penalties that can be imposed for the most serious offences.

The Companies Act (previously the Company Law Reform for Audit, Investigation and Community Enterprise), which is likely to be ratified in mid 2007, is of particular interest. Although some of the more controversial elements have been removed, it still contains a number of requirements that will fundamentally change the way that directors report the operations of their business.

This Act is considered to be the UK equivalent of 'Sarbanes-Oxley'. It will place new financial and audit controls on to companies and require company directors to sign off accounts on the basis that there is "no relevant financial information of which the auditors are unaware". It is not specifically aimed at IT systems, but inevitably it will involve tighter controls on the movement and storage of data and will therefore be a requirement of the IT department to ensure that this is achieved.

The Regulation of Investigatory Powers Act is also set to have a big impact on IT security in 2007, with the requirement for businesses to securely store all encryption keys and where necessary, make them available to the authorities in the event of criminal investigation.

Standards bodies have also reflected the maturing IT market with the introduction of new areas to established codes of practice, such as the proposed security metrics and measurements



## The Emerging Standards: ISO27004 and BS25999

---

standard (ISO27004, part of the ISO 27XXX Information Security Series) and the new business continuity management standard BS25999 (replacing PAS56).

With this new legislation in mind, how can corporate IT management be improved to accommodate these anticipated changes and make it even more relevant to the running of a modern 21<sup>st</sup> century business?

The answer lies in the continued development of our understanding of how IT, and in particular issues relating to security and performance, affect the day-to-day running of a company and the pivotal role played by IT departments.

This paper is concerned with the role that the emerging ISO27004 and BS25999 standards will have on IT departments; how they can be used to comply with new legislation and provide meaningful data to justify investment, demonstrating the financial benefits of effective IT systems and security policies.

Taken at face value, there does not seem to be an obvious link between the use of security metrics and the implementation of a business continuity management policy. However, if you dig a little deeper, some of the connections become more apparent.

As will be seen in this white paper, the cornerstone of ISO27004 is ISO27001, which is concerned with information security management in general. To achieve compliance to ISO27001, a company has to demonstrate that it has an effective business continuity management framework. BS25999 is the most up-to-date standard for business continuity and is therefore considered to be a reliable source of the current best practices.

At the heart of both standards is the desire to improve business practices. There are also considerable fringe benefits to be gained for the business as a whole and from the ability to deliver a higher quality service to customers.



## The Emerging Standards: ISO27004 and BS25999

---

### 2. Security Metrics and Measurements

Metrics are tools designed to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant performance-related data. IT security metrics must be based on IT security performance goals and objectives [1].

Attempts to measure IT performance using statistics are not new and in recent years have received a fair amount of bad press. There have been accusations that they can be 'gamed' or manipulated, which of course is possible with any form of statistic (to quote Mark Twain, although the words are thought to be attributed to the British prime minister Benjamin Disraeli, "There are lies: damn lies and statistics").

Supporters of metrics have often countered the argument by stating that a reliance on just opinion or experience can be easily tainted by unscrupulous practitioners relying heavily on the FUD (Fear, Uncertainty and Doubt) principle. This is equally as damaging to the process of measuring the effectiveness of IT security and systems. It adds no value when attempting to calculate the impact of the loss or interruption of key IT systems or the investment required to secure the systems in the first place.

Although these two views are a simplistic interpretation of the pros and cons of metrics, they do highlight the need to be very clear regarding what statistical measurements should be taken, the reliability and integrity of that data and the purpose for which such metrics will be used.

The science of security metrics has continued to develop over the past few years to such an extent that it is now deemed worthy of its own draft ISO standard (ISO / IEC27004). This has been integrated into the revised information security management standard ISO27001. Respected organisations such as the National Institute of Standards and Technology (NIST) in the United States have also made significant contributions to the production of guidelines and definitions on the use of security metrics.[1] [2] [3]

[1] NIST SP 800-55 Security Metrics Guide for Information Technology Systems

[2] NIST (Draft) SP 800-80 Guide to Developing Performance Metrics for Information Security

[3] NIST SP 800-26 Security Self Assessment Guide for Information Technology Systems



## The Emerging Standards: ISO27004 and BS25999

---

It is the ISO recognition however, that is most likely to lead to a marked increase in the use of security metrics and measurements in the United Kingdom. It would therefore seem prudent to be aware of what metrics can help achieve and their potential value to the business community.

### 2.1 What Metrics should be used?

In order to create meaningful metrics, it is necessary to properly define their scope and purpose. Well designed metrics can be used to provide assistance in the successful management of a wide range of IT security management issues such as:

- The satisfaction of legislative and regulatory requirements.
- The adherence to internal procedures.
- The measurement of progress in achieving goals and objectives.
- The justification of budgets and investment.
- The promotion of the effectiveness of training and awareness programmes.

It is hoped that the final ISO27004 document will define a series of core metrics that will be required to demonstrate adherence to the new standard. There should also be guidance for the creation of customised metrics and measurements.

If core metrics are defined, then one advantage would be the potential to collect industry wide statistics, allowing individual companies to benchmark their performance and progress. The ability to benchmark and obtain some form of statistical rating has long been the goal of many businesses and governments, particularly those involved with risk management and disaster recovery. However, enthusiasm must be tempered by the, as yet unknown, quantity and quality of the metrics that could be used. To be successful, it would also require widespread industry acceptance and agreement on the metrics to be used and the collection of statistics. Experience suggests that in practice, this will be difficult to achieve.

Another important consideration is to remember that the use of metrics and measurements should be seen as a complimentary exercise and not used to the complete exclusion of other more accepted methods for the gathering of business critical information and decision making. The use of metrics and statistics in isolation could create a false sense of security.



## The Emerging Standards: ISO27004 and BS25999

---

Many of the problems associated with numerical assessments have come from the practice of attributing arbitrary values to certain outcomes. The US Government's desire to assign a risk assessment 'score' to all travellers entering or leaving the country, based on a complex value-based system (the US Customs Automated Targeting System), is a good example of the over reliance on statistical measurements. As Bruce Schneier [4] commented: "In 2005 Customs and Border Protection processed 431 million people. Assuming an unrealistic model that identifies terrorists (and innocents) with 99.9% accuracy, that's still 431,000 false alarms annually." Clearly this would lead to huge problems and delays when travelling. Any seasoned IT security professional will be well versed with the problem of invasive security models and the amount of resentment it can cause amongst end users.

Where security metrics and measurements must seek to distance themselves from such criticism is to ensure that the statistics gathered are quantifiable and not arbitrary values.

### 2.2 IT Security Metric Example

For this example, we will look at the measurement of the effectiveness of an anti virus and software patching policy. The purpose of this will be to assess the companies' risk exposure to malicious software attacks such as viruses, trojans and worms. However, to actually collect the information will require that the company has in place a number of controls, including:

- Written policy for the use of anti virus software and patch management.
- A clear definition of the scope of the devices to be monitored (i.e. desktop PCs or Internet-facing servers).
- Appropriate audit software to collect the statistics.
- Defined roles and responsibilities for those staff tasked with collecting and analysing the information.
- The identification of any weaknesses or exclusions that could affect the information collected.
- A clear objective with criteria for determining success or failure.

[4] CRYPTO-GRAM, January 15 2007



## The Emerging Standards: ISO27004 and BS25999

---

The company has collected information from various departments, relating to the number of PCs that have up-to-date anti virus signatures and software patch levels.

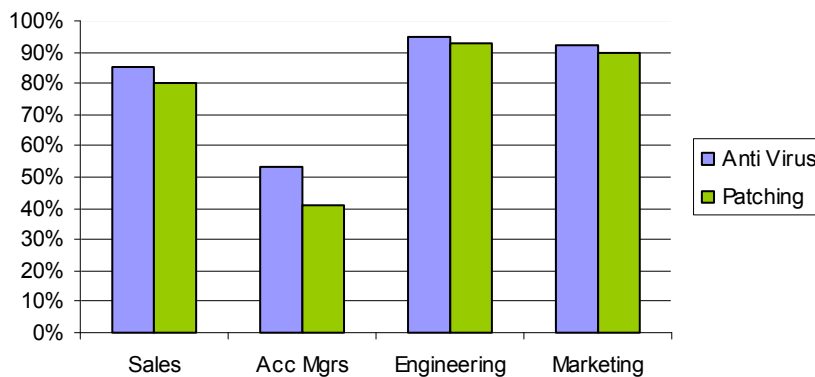


Figure 1: Example of company-wide patching and anti virus software use

Previous risk assessment exercises conducted by the company have established the requirement that a minimum of 92% of all PCs must be running an up-to-date anti virus signature database and that all applicable security patches must be installed in order to achieve a significant reduction in exposure to virus attacks. From the chart in Figure 1 it is clear to see that there is a problem with the account managers and they are significantly below the required level.

Further investigation might reveal that as a largely mobile workforce, these employees rarely connect to the main company network and are not receiving updates. Therefore the collection of this information will allow the IT department to direct additional resources to address the issue. This may take the form of improved education for the employees, the addition of local software controls to help automate updates whilst not connected to the corporate network and / or a change to the network access policy that enforces minimum levels of software and patch revision levels.



## The Emerging Standards: ISO27004 and BS25999

---

The results could also be used in conjunction with additional metrics, such as the plotting of actual virus incidents against departments, to identify an increased risk exposure that could be directly attributable to the poor level of patching and anti virus software observed. Budgetary discussions to justify the purchase of additional equipment to enforce the new policy could also be heavily influenced by the use of these metrics.

### 2.3 What Metrics Do Not Tell You

While security metrics will provide businesses with the opportunity to calculate valuable statistics, they are not suited to every purpose. It can be tempting to over play their importance. It is natural to focus on those issues where a value can be calculated and therefore it is easy to place a higher priority on them. Just as playing on fear, uncertainty and doubt is damaging and unhelpful, so is an over reliance on quantitative data.

Where it is possible to calculate a metric, it is important to guard against attempts to manipulate those figures by simply carrying out limited or misguided actions designed to improve the metric value. Such actions may make the figures look better, but they could leave the company with a false sense of security and ultimately, unprotected against critical security threats.

If the question is: “How secure is my business?”, then security metrics alone will not provide the answer. If, however, the objective is to ascertain the exposure of your company to a virus attack, then well chosen and measured security metrics will be able to help.

### 2.4 Security Metrics Conclusion

Even from the relatively simple example in this paper, it is easy to see that the decision to implement a programme of metrics and measurements is not one to be taken lightly. The quality of the results will be directly attributable to the integrity and accuracy of the raw information collected and of course, the stated objectives of the metric framework. It also becomes clear why ISO27004 has been designed to be implemented as part of the wider ranging ISO27001 information security management standard; as companies will need to ensure that their information gathering infrastructure meets or exceeds industry-recognised standards to withstand scrutiny from auditors and accountants.



## The Emerging Standards: ISO27004 and BS25999

---

The use of security metrics and measurements is highly likely to increase. Properly researched and implemented, they will prove to be a valuable resource for IT security officers and the company as a whole. Poorly implemented, they will provide meaningless figures, which may result in infrastructure weaknesses and a perceived false sense of security. Effective policies and procedures will be the cornerstone for reliable security metrics and measurements.



## The Emerging Standards: ISO27004 and BS25999

---

### 3. BS25999 Business Continuity Management (BCM)

Business Continuity Management (BCM) is a business owned, business driven, process that establishes a fit-for-purpose strategic and operational framework to ensure that a business can continue to function in an effective manner following a major incident or outage [5].

The purpose of BS25999 is to provide a basis for understanding, developing and implementing business continuity within an organisation and to provide confidence in business-to-business and business-to-customer dealings. It also enables the organisation to measure its BCM capability in a consistent and recognised manner.

The Standard will consist of two parts:

- BS25999-1 Code of Practice.
- BS25999-2 Specification.

BS25999-1 is based heavily upon the BS PAS56 document (which it has now superseded). It is a code of best practice and recommendations for implementing a BCM framework.

BS25999-2 is a new publication, known as the 'Specification for Business Continuity Management'. Company certification to BS25999 will eventually be made using this document as the framework for assessment.

The time table for publication is flexible. At present, BS25999-1 has been published (November 2006), with part 2 following in 2007. Although part 2 is not yet available (and therefore official certification to the Standard is not yet obtainable), this should not deter any company from implementing a BCM framework using the part 1 guidelines. Business continuity planning is an essential, but often overlooked, part of modern company operations.

This section of the white paper is concerned with the perceived impact and benefit that the new standard could bring to a company, should it be adopted.

[5] BS25999-1 Definition



## The Emerging Standards: ISO27004 and BS25999

---

### 3.1 Implementing a BCM Solution

If a business does not already have disaster recovery (DR) or BCM policy in place, then why should it consider BS25999? The ability to continue trading in the event of an unforeseen incident should be a fundamental part of any business plan. There are many threats that could affect the business, from natural disasters to security incidents (both physical and logical). The location, nationality and type of business could also make a company a target.

For those companies operating in high-risk areas, a business continuity plan is not an option: it is an essential part of their business operations.

#### 3.1.1 BCM Lifecycle

BS25999 specifies a lifecycle approach to promote the benefits of BCM and to ensure that it becomes part of the company culture:

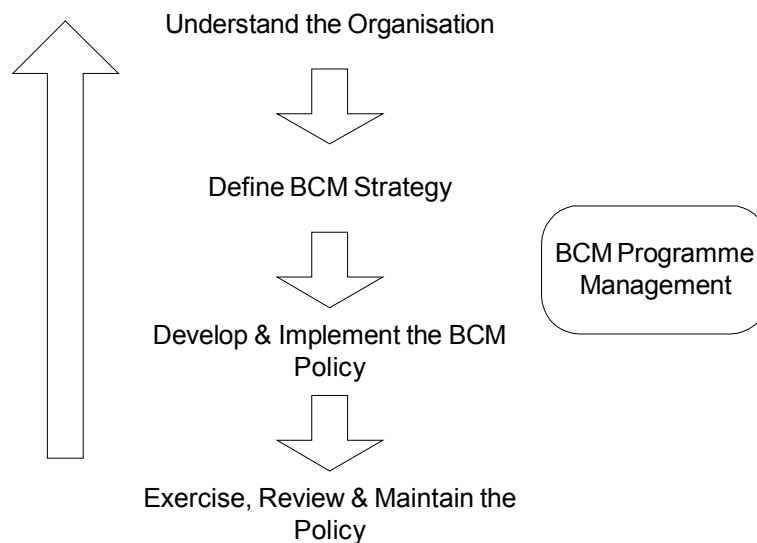


Figure 2: Business Continuity Management Lifecycle

The BS25999 approach is not to see BCM as a one-off exercise. To be truly successful, it must be embraced by the whole company. The plan must be kept up-to-date and regularly reviewed



## The Emerging Standards: ISO27004 and BS25999

---

to ensure that it remains current and applicable. Senior management should be assigned to oversee and run the BCM Programme Management function.

Perhaps the most important part of implementing a BCM framework is to carry out an exercise to test the plan. By not testing to see whether the plan actually works, an organisation runs the serious risk of negating the time, effort and money invested in the BCM framework. It is also one of the reasons that the myth of BCM as an 'investment with no return' is perpetuated.

The completion of a thorough test serves as an effective training exercise for all members of staff and helps them to understand the need for BCM and its importance to the company. Again, this is not a one-off exercise. While company policies rarely change significantly, the actual plan may and regular testing is the most effective way of determining its suitability and accuracy.

BCM is often seen as a largely IT-related task; a lot of the effort required to ensure continued trading after a serious incident, will be directed towards technology (the restoration of telephone systems, PCs, network devices, servers and critical data for example).

Whilst this is certainly true, an effective BCM policy should also consider areas such as:

- Logistics and Supply Chain.
- Government Regulations.
- Impact on Reputation.
- Transportation.
- Key Personnel.

### 3.1.2 Logistics and Supply Chain

The effects of a serious outage can cause problems not just for the company, but also its suppliers. Will it be possible for your suppliers to reach your disaster recovery site and deliver goods? What impact on manufacturing would an outage have? It is important that you discuss these issues with your key suppliers so that plans can be drawn up to continue to supply goods as required.



## The Emerging Standards: ISO27004 and BS25999

---

### 3.1.3 Government Regulations

Aside from the regulations that may affect your business on a day-to-day basis, companies should be aware of the wide ranging powers that the authorities can now use in the event of a major disaster. For the United Kingdom, the government could invoke emergency powers under the Civil Contingencies Act 2004. Although this is only likely to be used in the event of a major event (such as terrorist activity), the Act allows for a defined area to be evacuated or people could be prevented from leaving a defined area. From a BCM perspective, this could either prevent staff from reaching a disaster recovery site or restrict the movements of key individuals.

### 3.1.4 Impact on Reputation

The inability to continue trading after a major incident is potentially disastrous to any company. Customer loyalty will be severely tested and in many cases may do irreparable damage to a company's reputation. The positive side of an effective BCM framework and the ability to keep trading in the event of a serious incident may mean that the company gains additional customers.

### 3.1.5 Transportation

Being able to move staff quickly to a disaster recovery site will be essential to those businesses with large scale operations. It may be possible to equip many staff with 'home offices' and allow them to work remotely.

### 3.1.6 Key Personnel

As part of the initial planning for a BCM solution it will be necessary to identify the key staff that will be essential to the continued running of the company during a crisis. Consideration should be given to equipping those staff with pagers or similar devices to ensure availability.

While this list is not mean to be exhaustive, it does enable you to comprehend the level of planning that is required to implement an effective BCM solution. BS25999 stresses the need for BCM to be embedded into the culture of an organisation and not left as an exercise for IT to complete. In fact, IT should play a support role in the BCM framework, which should ultimately be driven by senior management.



## The Emerging Standards: ISO27004 and BS25999

---

### 3.1.7 Overcoming Objections to BCM

Business Continuity Management has traditionally suffered from two main problems:

- Lack of Board Level Recognition.
- An Investment with No Return.

### 3.1.8 Lack of Board Level Recognition

To have any chance of success, a BCM framework must have the support of the senior executives in the company. Inevitably, implementing BCM will involve the investment of considerable amounts of time and money. It may also require the company to change the way it works and appoint new staff.

It is essential that the board understands the risks that they face and the impact to the business if they are unable to adapt and continue trading in the event of a major incident. The benefits to implementing a proper BCM framework (detailed below) must be highlighted to them.

### 3.1.9 An Investment with No Return

The reason often stated for the lack of a proper BCM framework is the large cost associated with the implementation; there often exists a perception that there is little or no return on such an investment. However, this view is somewhat short sighted and it is important to understand the benefits that BCM can bring to a business. These include:

- Enabling the business to respond quickly and effectively to significant disruption.
- Enhance reputation by handling crisis situations effectively and without disruption.
- Promote good management practices and due diligence throughout the company.
- Make the company more resilient and better able to service clients in the event of an emergency.
- May lower insurance costs by being able to demonstrate the completion of risk assessment exercises.



## The Emerging Standards: ISO27004 and BS25999

---

### 3.2 BS25999 Conclusion

Without doubt, BS25999 is set to become one of the most important standards produced in recent years. There has already been considerable interest in the Standard, witnessed by the large number of downloads (estimated to be 20 times that of most of the other British Standards).

What BS25999 establishes, along with security metrics and measurements, is that to be successful, it will require senior management support and it must be built on a foundation of strong policies and procedures.

The requirement for businesses to improve their financial accountability (under the terms of legislation such as the new Companies Act) will mean that changes will inevitably be made to how data is collected and stored. A competent BCM strategy and framework, such as one based on BS25999, that ensures that all data is properly protected and can be retrieved in the event of a major incident, will be essential to demonstrating that businesses are taking their responsibilities seriously.



# The Emerging Standards: ISO27004 and BS25999

---

## Appendix A

### References

#### Security Metrics and Measurements

- National Institute of Standards and Technology (NIST) – <http://www.nist.gov>
- Securitymetrics.org – [www.securitymetrics.org](http://www.securitymetrics.org)

#### BS25999

- BS25999-1:2006 British Standards – <http://www.bsi-global.com/en/>

Readers of this white paper are also encouraged to visit the following sites:

- The Business Continuity Institute – [www.thebci.org](http://www.thebci.org)
- IT Infrastructure Library (ITIL) – [www.itil.co.uk](http://www.itil.co.uk)
- The Institute of Risk Management – [www.theirm.org](http://www.theirm.org)

### Acknowledgments

This white paper was written by Chris Leppard MBCS, CISSP, and Technical Account Manager at Corsaire.

### About the Author

Chris has more than 15 years experience in IT and IT security, working in both technical and sales capacities. His career has taken him from the banking industry to major Telco's and specialist security consultancies. In recent years he has concentrated on technical sales, providing complex IT security solutions to a number of FTSE 250 clients.

### About Corsaire

Corsaire are experts at securing information systems, consultancy and assessment. Through our commitment to excellence we provide a range services to help organisations protect their information assets and reduce corporate risk.

Founded privately in the United Kingdom in 1997, we operate on an international basis with a presence across Europe and the Asia-Pacific rim. Our clients are diverse, ranging from



## The Emerging Standards: ISO27004 and BS25999

---

government security agencies and large blue-chip FTSE, DAX, Fortune 500 profile organisations to smaller internet start-ups. Most have been drawn from banking, finance, telecommunications, insurance, legal, IT and retail sectors. They are experienced buyers, operating at the highest end of security and understand the differences between the ranges of suppliers in the current market place.

For more information contact us at [contact-us@corsaire.com](mailto:contact-us@corsaire.com) or visit our website at <http://www.corsaire.com>