

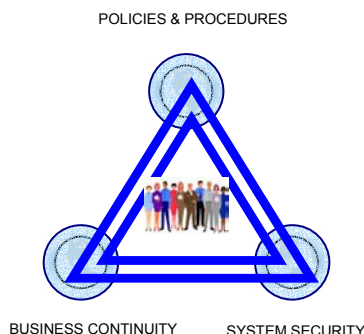


**Operational Risk – Definitions**

Operational risk is a term frequently associated with the financial markets and the work of the Basel Committee on banking supervision. But it has also come to take on a wider significance and is more broadly defined as the risk of loss caused by deficiencies in information systems, business processes or internal controls, as a result of either internal or external events.

For the purpose of this paper it is the broader definition that is being considered. In this context, operational risk involves breakdowns in internal controls and corporate governance, such that those breakdowns can lead to financial losses through error, fraud, failure to perform in a timely manner, or cause the interests of the business to be compromised in some other way.

There are three main influences affecting operational risk; a company’s policies and procedures for transacting business, the means by which the company can sustain its operations in the event of an interruption (business continuity), system security and the roles and responsibilities of the employees, management and shareholders in terms of their authentication and authorisation to execute business on behalf of the company.



The argument follows that there is an integral relationship between these influences and therefore a need to address them together. It also follows that there is a collective opportunity to mitigate or minimise the effect of these influences causing an interruption to the business, whether this is through external or internal events.

To create the foundation for a solution, we have taken a high level overview of the options for business continuity and system security that are available today and how together they can be deployed to protect a company’s systems from disruptive events.

**Business Continuity**

Business continuity management can be defined as 'the processes, procedures, decisions and activities to ensure that an organisation can continue to function through an operational interruption'. The aim of a business continuity plan is to achieve a cost-effective contingency solution that balances the value of potential losses to the business and its assets, against the cost of guaranteeing continuity of critical business processes. The task is to ensure, that in the event of an interruption, a minimum level of service can be provided to the customer with a perception of business as usual.

There are typically six steps to developing a business continuity plan that comprise; risk assessment, event impact analysis, strategic planning, implementation, testing and maintenance.

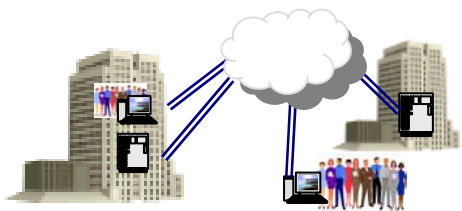
- Risk Assessment – a realistic appraisal of events that could occur and their associated risks
- Event Impact Analysis – the possibility of the event occurring and its potential impact
- Strategic Planning – definition of critical risks, ways to migrate and protective measures
- Implementation – documentation and publication of the business continuity plan
- Testing – theoretical ‘what if?’ scenario tests and activation of systems support
- Maintenance – ongoing refinement and update to reflect new risks and circumstances



Today, many of the perceived risks to business continuity are security related and in the risk assessment step above it is important to consider what potential breaches of system security might occur, what impact they might have on the business and how one might mitigate against them.

### **System Security**

The specific focus here is the protection of the company's information assets, the individual roles and responsibilities of the company's employees in accessing those assets and the external access to those assets by external resources (people and systems), either legitimately or otherwise.



The security aspects considered here include:

- Employees accessing internal systems and external resources
- Internal systems directly accessing external resources (either in the company's domain) or external to the company (suppliers, customers)
- External resources whether individuals or systems accessing the company's systems

This paper reviews the practical security issues and highlights some of the technology solutions that can be used to build a secure environment and one that will form part of a business continuity plan.

### Employees accessing internal systems and external resources

Access to all commercial applications is normally through at least a user id and password, although higher more secure levels of access are becoming increasingly desirable, particularly when they involve significant value transactions. Equally where access is required to multiple applications, the concept of a single sign-on also becomes important to avoid the necessity to maintain multiple passwords for different applications. For example, the use of a multi-platform, common authentication process can secure an organisation's intranet and extranet against inside and outside threats, even when using unsecured networks (such as the Internet). These solutions are scalable and interoperable and can provide flexibility through their support for multiple authentication mechanisms; passwords, certificates, token cards and smart cards. Today many applications are becoming web-based and web authentication solutions have so far utilised a user ID and password and/or a client certificate that is unlocked with a PIN code for higher security. It is now possible to take this authentication a stage further, so that the web server can delegate users' credentials to secure applications behind it (e.g. a database). This can then ensure end-to-end security and common authentication across the entire application architecture. With the increasing usage of wireless devices, it will become even more important to create a secure access infrastructure that can be protected against unauthorised access and intrusion.

While this deals with the authentication of the user to access applications and services, increasingly it is necessary to classify electronically information and data within a company. It might be desirable for a user to be able to access certain information, but to be constrained from changing it, or distributing it outside the company without the appropriate permission.



We have referred to protecting the company's assets and there is an argument that all sensitive data should be centrally stored, maintained and properly backed-up. And yet in many cases today this data can be found on a user's desktop without security or proper back-up. The issue becomes not only the right of the user to access the application or data through authentication, but also the authority of the user to read, update and distribute the data.

Where applications and data are centrally maintained, setting roles, responsibilities and levels of permissions for users gives added security. For example, where data can be downloaded from the web it can be restricted to that which is necessary for users to perform their tasks. Equally, controls can be put in place to ensure that only authorised individuals can distribute sensitive data.

### Internal systems directly accessing external resources

In this scenario a company's applications might be accessing external resources and applications, possibly within the company's domain and this may be through a virtual private network to other physical locations. This could extend to suppliers and customers who might be part of that private network, or who have access to it through a public network.

All these disparate applications, services and data must be properly secured and may have to take account of Storage Area Networks, the need for High Availability, archiving, back-up and recovery solutions.

The task is to create and maintain a secure and managed network environment that is resistant to unauthorised interruption and one whereby the company's data is protected.

### External resources whether individuals or systems accessing the company's systems

The converse of the above and to some extent more difficult to predict, but the principles of authentication and authorisation

remain valid for individuals and other system resources such as customers and suppliers gaining access to the company's systems.

### **Integrated Approach to Operational Risk**

It has been argued that there is an integral relationship between the policies and procedures that a company defines for the operation of its business, the ability to keep that business running in the event of a disruption and the security of the company's applications and data. While any association between these three elements is only part of managing operational risk, they are none-the-less fundamental to minimising the risk of loss caused by deficiencies in information systems, business processes or internal controls, that might result from either internal or external events.

By taking an integrated approach it is much more likely, that for those areas where there is interdependency between policies and procedures, business continuity and security, that a sound and workable solution will be found.

### **Software Solutions for Operational Risk**

It is unlikely that any one software solution will address all aspects of operational risk. Designing and implementing a solution will require several software components to manage security authentication and authorisation, business continuity and corporate knowledge management. These are some of those components and there will be others that need to be considered in an overall solution.

InitioStar has been evaluating a number of software suppliers with an objective to create a packaged infrastructure solution for managing Operational Risk. The delivery of such a solution will be probably be through a systems integrator or a specialist software house as they will have the skills to package, tailor and implement this type of solution.