EXECUTIVE WHITE PAPER
BY JOHN SHERWOOD, CISSP

SABSA® SECURITY ARCHITECTURE

SABSA®

SABSA® is the Sherwood Associates Business Security Architecture methodology. Following the integration of Sherwood Associates Limited into Netigy Corporation, this methodology has become an important part of the Netigy consulting methods collateral. This document introduces some ideas on architecture and describes the SABSA® approach.

THE ORIGINS OF ARCHITECTURE

Architecture has its origins in the building of towns and cities, and we all understand this sense of the word, so let us begin by examining the meaning of 'architecture' in this traditional context.

Architecture is a set of rules and conventions by which we create buildings that serve the purposes for which we intend them, both functionally and aesthetically. Our concept of architecture is one that supports our needs to live, to work, to do business, to travel, to socialise and to pursue our leisure. The multiplicity and complex interaction of these various activities must be supported, and this includes the relationship between the activities themselves and their integration into a whole lifestyle. Architecture is founded upon an understanding of the needs that it must fulfil.

These needs are expressed in terms of function, aesthetics, culture, government policies and civil priorities. They take into account how we feel about ourselves and about our neighbours, and how they feel about us. In these various ways, architecture must serve all those who will experience it in any way.

Architecture is also both driven and constrained by a number of specific factors. These include: the materials available within the locale that can be used for construction; the terrain, the prevailing climate; the technology; and the engineering skills of the people.

This all boils down to three major factors that determine what architecture we will create. These factors are:

- Our goals;
- The environment;
- Our technical capabilities.

INFORMATION SYSTEMS ARCHITECTURE

This concept of 'architecture' has been adapted to areas of life other than the building of towns and cities. For example we talk about a 'naval architect' being someone that designs and supervises the construction of ships. In more recent times we have adopted the term in the context of designing and building business computer systems, and so we have introduced the concept of 'information systems architecture'.

In the same way that conventional architecture defines the rules and standards for the design and construction of buildings, information systems architecture addresses these same issues for the design and construction of computers, communications networks and the distributed business systems that we implement with these technologies.

As with the conventional architecture of buildings, towns and cities, information systems architecture must therefore take account of:

- The goals that we want to achieve through the systems;
- The environment in which the systems will be built and used;
- The technical capabilities that we have to construct and operate the systems and their component sub-systems.

If we accept this analysis then we are already well on the way to recognising that information systems architecture is concerned with much more than mere technical factors. It is concerned with what we want to achieve and with the environmental factors that will influence those achievements.

Unfortunately the reality is that in many organisations this broad view of information systems architecture is not understood. Technical factors are often the only ones that influence the architecture, and so the architecture fails to de-

liver what the business expects. The relationship between the IT division of the organisation and the business divisions is therefore often very strained. The business sees the IT service group as being like a large black hole into which you pour large amounts of money, with little benefit ever being delivered back in return. The IT people do not have the right level of insight and understanding to know what is wrong, and so they plough on with their misguided approach, trying to devise better and better technical solutions to keep their business colleagues and masters happy. It is a doomed relationship.

So, we hear many people using the term 'information systems architecture' but few of them understand what it means. In this document we are concerned only with one aspect of information systems architecture: that is the security of business information systems. However, we shall strive to avoid the classical mistakes that are made when one concentrates only on the technical capabilities and neglects the goals and the environment. We shall therefore talk about an 'enterprise security architecture', to emphasise that it is the enterprise and its activities that we are securing, and that the security of computers and networks is only a means to this end.

ENTERPRISE SECURITY ARCHITECTURE

It is the experience of many corporate organisations that information security solutions are often designed, acquired and installed on a tactical basis. A requirement is identified, a specification is developed and a solution is sought to meet that situation. In this process there is no opportunity to consider the strategic dimension, and the result is that the organisation builds up a mixture of technical solutions on an *ad hoc* basis, each independently designed and specified and with no guarantee that they will be compatible and interoperable. Worse still, there is no analysis of the long-term costs, especially the operational costs, and there is no strategy that can be identifiably said to support the goals of the business.

It does not have to be this way. The solution lies in the development of an enterprise security architecture which is business-driven and which describes a structured interrelationship between the technical and procedural solutions to support the long-term needs of the business of the organisation. If the architecture is to be successful, then it must provide a rational framework within which decisions can be made upon the selection of security solutions. The decision criteria should be derived from a thorough understanding of the business requirements, including:

- the need for cost reduction
- modularity, scalability
- re-usability
- operability
- usability
- inter-operability both internally and externally
- integration with the enterprise IT architecture and its legacy systems.

Furthermore, IT security is only a small part of information security, which in turn is but one part of a wider topic: business security. Business security embraces three major areas: information security; business continuity; physical and environmental security. Broader still is the view that business security is concerned with all aspects of operational risk management. Only through an integrated approach to these broad aspects of business security will it be possible for the enterprise to make the most cost-effective and beneficial decisions with regard to the management of operational risk. The enterprise security architecture and the security management process should therefore embrace all of these areas.

At Netigy Corporation (and before that at Sherwood Associates Limited) we have been working for some years (since 1995) with a model for enterprise security architecture. This model, known as SABSA® is the basis that we have used for major consulting assignments with our clients, and over the years we have been reviewing and refining our methodology in the light of experience and in response to new inputs of ideas from various sources.

The primary characteristic of this model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. The model is layered, with the top layer being the business requirements definition stage. At each lower layer a new level of abstraction is developed, going through the definition of the conceptual architecture, logical architecture, physical architecture and finally at the lowest layer, the selection of technologies and products (component architecture) - in other words, the shopping list. In addition the whole area of security management, administration and operations is addressed through the operational architecture.

The model itself is generic and can be the starting point for any organisation, but by going through the process of analysis and decision-making implied by its structure, it becomes specific to the enterprise, and is finally highly customised to a unique business model. It becomes in reality the *enterprise security architecture*, and it is central to the success of a strategic programme of information security management within the organisation.

WHY ARCHITECTURES SOMETIMES FAIL TO DELIVER BENEFIT

HISTORICAL BACKGROUND

For many years corporate organisations have been implementing technical solutions to business security requirements on a very tactical basis. Usually a requirement is identified and a product is sought and acquired to meet that requirement without regard to the broader implications. A point solution is implemented which is often effective in providing some security, but frequently no-one is really sure that the security is appropriate to the risk, or that the cost is commensurate with the benefit, or that it meets a wide variety of other business requirements which are not specifically risk-related.

This can lead to many problems. The solutions are often isolated and incapable of being integrated together or of interoperating with one another. The variety of solutions leads to increased complexity and cost of support, and in particular can lead to an exploding workload with regard to administration and management. Worst of all, because there has been inadequate attention paid to the business requirements, the "solution" often hinders the business process rather than helping it, and the reputation of "security" among the business community gets worse and worse.

Appropriate 'business security' is that which protects the business from undue operational risks in a cost-effective way. If 'business security' is to be effective in enhancing the business process and achieving business goals (and what other possible use could it have?) then the approach described above cannot continue. A much more strategic view should be developed, in which the business requirements are the primary driver for developing effective information security solutions.

THE WIDER BUSINESS REQUIREMENTS

For the moment let us return to the issue of information security, using it as an example, whilst remembering that our requirements for business security and operational risk management also span the areas of business continuity and physical and environmental security. The same principles developed below can be applied across the entire area of business security.

The primary business requirements for information security are business-specific. They will usually be expressed in terms of protecting the availability, integrity, authenticity and confidentiality of business information, providing accountability and auditability in information systems, and providing assurance to the management team that all this has been achieved. To understand these requirements, a detailed analysis of the business processes is required, using as source data information gathered by direct interviews with operational business managers.

However, there is much more to the business requirements than pure "security and control". Information security provides for the *confident use of information for business purposes across the entire organisation*. The generic business requirements for an information security solution often include the following:

USABILITY

Is the solution appropriate to the technical competence of the intended users and will it be ergonomically acceptable to those users?

INTER-OPERABILITY

Will the solution provide for the long-term requirements for inter-operability between communicating information systems and applications?

INTEGRATION

Will the solution integrate with the wide range of computer applications and platforms for which it might be required in the long term?

SUPPORTABILITY

Will the solution be capable of being supported in the environment[1] within which it has been designed to be used?

LOW COST DEVELOPMENT

Is the solution of modular design and hence capable of being integrated into a development programme at minimal cost?

FAST TIME TO MARKET

Is the solution capable of being integrated into a development programme with minimal delay?

SCALABILITY OF PLATFORMS

Will the solution fit with the range of computing platforms[2] with which it might be required to integrate?

SCALABILITY OF COST

---

[1] Including the number of end-users and service-delivery points, their geographical location and their distribution.

[2] Potential platforms range from high-end mainframes, through mid-range NT & UNIX boxes and AS/400, down to PCs and work-stations.

Is the entry-level cost appropriate to the range of business applications for which the solution is intended?

SCALABILITY OF SECURITY LEVEL

Does the solution support the range of cryptographic and other techniques that will be needed to implement the required range of security strengths?

RE-USABILITY

Is the solution re-usable in a wide variety of similar situations to get the best return on the investment in its acquisition and development?

OPERATIONS COSTS

Will the cost impact on systems operations be minimised?

ADMINISTRATION COSTS

Will the solution provide an efficient means for security administration to minimise the costs of this activity?

RISK-BASED COST / BENEFIT EFFECTIVENESS

Is the reduction of risk (the benefit) appropriate to the costs of acquisition, development, installation, administration and operation?

ENABLING BUSINESS

Finally there are usually a number of business-specific requirements which influence the security strategy. These include requirements where security has an important role in generating the appropriate level of confidence so as to enable new ways of doing business using the latest advances in information technology, such as:

- Exploiting the global reach of the Internet;
- Outsourcing networks and computer systems;
- Providing remote access to third parties;
- Developing on-line business services;
- Obtaining software upgrades and system support through remote access by vendors;
- Tele-working, 'mobile computing', 'road warriors' and the 'virtual office'.

FIGHTING AGAINST FAILURE

Unless the security architecture can address this wide range of operational requirements and provide real business support and business enablement, rather than just focusing upon 'security and control', then it is likely that it will fail to deliver what the business expects.

This type of failure is a common phenomenon throughout the information systems industry, not just in the realm of information systems security. In using the SABSA® approach our whole emphasis is on the need to avoid this mistake, by keeping in mind at all times the real needs of the business. It is not sufficient to compile a set of business requirements, document them and put them on the shelf, and then proceed to design a security architecture driven by technical thinking alone. Being a successful security architect means thinking in business terms at all times, even when you get down to the real detail and the nuts and bolts of the construction. You always need to have in mind the questions: Why are we doing this? What are we trying to achieve in business terms here? Otherwise you will lose the thread and finish up making all the classic mistakes.

It will also be difficult to battle against the numerous other people around you who do not understand strategic architecture, and who think that it is all to do with technology. These people will constantly challenge you, attack you and ridicule you. You have to be ready to deal with this. You have to realise that being a successful architect is also about being a successful communicator who can sell the ideas and the benefits to others in the enterprise who need to be educated about these issues.

One of the most important factors for success is to have buy-in and sponsorship from senior management levels within the enterprise. Enterprise architecture cannot be achieved unless the most senior decision-makers are on your side. The fruits of the architectural work will be enjoyed throughout the enterprise, but only if the enterprise as a whole can begin to think and act in a strategic way. Creating this environment of acceptance and support is probably one of the most difficult tasks that you will face in the early stages of your work.

SECURITY ARCHITECTURE NEEDS A HOLISTIC APPROACH

Many people make the mistake of believing that building security into information systems is simply a matter of referring to a checklist of technical and procedural controls and applying the appropriate security measures on the list. However, security has an important property that most people know about but few pay any real heed to it: it is like a chain, made up of many links, and the strength and suitability of the chain is only as good as that of its weakest link. At worst, if one link is missing altogether, the rest of chain is valueless.

The chain is a reasonably good analogy, but the problem is actually much worse than this.

Imagine a check-list that has the following items: engine block; pistons; piston rings; piston rods, bearings, valves; cam shaft, wheels, chassis, body, seats, steering wheel, gear-box, etc. Let us suppose that this list comprehensively itemises every single component that would be needed to build a car. If we go through the checklist and make sure that we have all of these components, does it mean that we have a car? Can we be sure that all the parts have been designed to work together as one smooth-running system? Does it give us any assurance that the car has been properly assembled, that the engine has been tuned, that it is actually running smoothly at this moment and that someone is at the controls governing the speed, lubricating the moving parts, maintaining its fuel supply and monitoring its performance? The answer is obviously in the negative, and so it is with security.

Checklists are not the entire answer. Security architecture needs a holistic approach:

- Do we understand the requirements?
- Do we have a design philosophy?
- Do we have all of the components?
- Do these components work together?
- Do they form an integrated system?
- Does the system run smoothly
- Are we assured that it is properly assembled?
- Is the system properly tuned?
- Do we operate the system correctly
- Do we maintain the system?

The analogy of the car as a complex system that needs a holistic architectural design is much more powerful than the idea of a chain. Security architecture is like the car, not the chain.

SECURITY ARCHITECTURE MODEL

A LAYERED MODEL OF ARCHITECTURE

To establish a layered model of how a security architecture is created, we shall return for a moment to the use of the word in its conventional sense: the construction of buildings.

We propose a six-layer model, the summary of which is in Table 1. It follows closely the work done by John A. Zachman in developing a model for enterprise architecture, although we have adapted it somewhat to our own view of the world. Each layer represents the view of a different player in the process of specifying, designing, constructing and using the building.

Table 1: Layered Architecture Views

The Business View	Contextual Architecture
The Architect's View	Conceptual Architecture
The Designer's View	Logical Architecture
The Builder's View	Physical Architecture
The Tradesman's View	Component Architecture
The Facilities Manager's View	Operational Architecture

There is another configuration of these six layers which is perhaps more helpful, shown in Figure 3. In this diagram we see that the 'operational security architecture' has been placed alongside the other five layers. This is because operational security issues arise at each and every one of the other five layers. Operational security has a meaning in the context of each of these other layers, and in the chapters on operational security architecture it is this view that we have used to structure the work.

THE BUSINESS VIEW

When a new building is commissioned, the owner has a set of business requirements that must be met by the architecture. At the highest level this is expressed by the descriptive name of the building: it is a domestic house; a factory; an office block; a sports centre; a school; a hospital; a warehouse; a theatre; a shopping centre; a multi-storey car park; or whatever. Each one of these business uses immediately implies an architecture that will be different from all the others, an architecture that will fulfil our expectations for the function of the building in business terms.

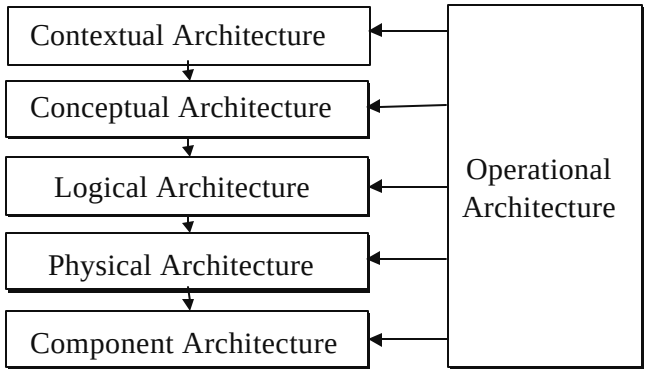

Figure 3: The SABSA® Model for Security Architecture

Having stated *what* sort of building is needed the owner must then decide some more detail about its use:

- *How* will it be used? The detailed functional description.
- *Where* should it be located, and what is its geographical relationship to other buildings and to the infrastructure (such as roads, railways etc)?
- *Who* will use the building, including the types of people, their physical mobility, the numbers of them expected, and so on?
- *When* will it be used? The times of day / week / year, and the pattern of usage over time.
- *Why* do we want this building? The goals that we want to achieve.

This type of analysis is essential before any type of design work is done. It is through this process that the requirements of the building are established, and understanding the requirements is a pre-requisite to designing a building that will meet those requirements.

When we architect a secure business system, the same applies. There are many possible architectural approaches that we could take, but the one that will be the most suitable will be driven from a clear understanding of the business requirements for the system.

- *What* type of system is it and *what* will it be used for?
- *How* will it be used?
- *Where* will it be used?
- *Who* will use it?
- *When* will it be used?
- *Why* will it be used?

These are the characteristic questions that we must ask. From the analysis of the replies that we receive we shall be able to gain an understanding of the business requirements for the secure system. From those we shall be able to synthesise a systems architecture and a security architecture that meets those requirements.

We call this business view the *contextual architecture*. It is a description of the business context in which our secure systems must be designed, built and operated.

Any attempt to define an architecture that takes a short cut and avoids this essential step is very unlikely to be successful. Even so, simple observation tells us that the majority of enterprises undertaking architectural work do not take this stage seriously. It is very common for systems architecture work to begin from a technical perspective, looking at technologies and solutions whilst ignoring the requirements.

It seems to be such obvious common sense that one must first understand the requirements, and yet so few people seem to know how to approach architecture development in the information systems arena. There is often a pervasive arrogance that makes technologists and technicians believe that they already know the requirements, even though they have a very poor relationship with those who might express these requirements.

The results of taking a short cut in the requirements definition stages of an architecture development are abundantly clear. Look around at most large corporate enterprises and at their information technology infrastructure managers or applications teams. What is the relationship between the business community and the IT community? In many cases it is barely concealed, open warfare. For many years the 'business people' have been complaining that the IT people are unable to deliver what the business needs, and that IT is a serious source of cost with very little tangible benefit to show for it. The reason is simple: the business people are right. Business IT development is very often driven by technological innovation, not by business needs. Those with responsibility for architecture and technical strategy fail to understand the business requirements because they do not know how to do otherwise. Ignorance of architectural principles is commonplace.

We describe here how to take a layered approach to security architecture development. Many of you will be tempted to flip the pages to get to the end sections where the solutions can be found. You are in a hurry, and whilst you know that this step-wise approach is correct, you simply do not have the time to linger on the appetisers and starters – you need to get to the meat course. Well, be warned. There simply is no substitute for doing architecture work the proper way. You may try to take short cuts, but your efforts will most likely result in failure, which costs the business more money, delivers less benefit, and destroys the confidence that business people may have in information technology as the means to enable business development.

In the model that we present here, the contextual architecture is concerned with:

- *What*? The business assets to be protected (brand, reputation, etc.) and the business needs for information security (security as a business enabler, secure electronic business, operational continuity and stability, compliance with the law, etc.).
- *How*? The business processes that require security (business interactions and transactions, business communications, etc.).
- *Where*? The location-related aspects of business security (the global village market place, distributed corporate sites, remote working, etc.).
- *Who*? The organisational aspects of business security (management structures, supply chain

structures, out-sourcing relationships, strategic partnerships).

- *When*? The time-related aspects of business security (business transaction throughput, lifetimes and deadlines, just-in-time operations, time-to-market, etc.).
- *Why*? The business goals, success factors and operational risks that drive the need for business security (brand protection, fraud prevention, loss prevention, legal obligations, business continuity, etc.).

THE ARCHITECT'S VIEW

An architect is a creative person with a grand vision. Architects thrive on challenging business requirements. They marshal their skill, experience and expertise to create an inspired picture of what the building will look like. They give us impressionistic drawings and high-level descriptions. The pictures are painted with broad brushes and sweeping strokes. They prepare the way for more detailed work later on, when other people with different types of expertise and skill will fill in the gaps with fine brush strokes.

The architect's view is the overall *concept* by which the business requirements of the enterprise may be met. Thus we also refer to this layer of our architectural model as the *conceptual architecture*. It defines principles and fundamental concepts that guide the selection and organisation of the logical and physical elements at the lower layers of abstraction.

When describing the enterprise security architecture, this is the place to describe the security concepts and principles that we shall use. These include:

- *What* we want to protect, including business information, business entities and their relationships.

Some of the most important of these concepts are *trust*, which is a business concept, and *information security*, which is a technical concept to support the trust that we develop between the parties to a business relationship. This leads us on to other concepts: business entities; business transactions between entities; entity identification, authentication and authorisation; and trusted third parties.

- *How* we want to achieve the protection, in terms of high-level technical and management *security strategies*.

These strategies set out the framework for individual tactical elements at the lower layers, ensuring that these fit together in a meaningful way to fulfil the overall strategic goals of the business. Such strategies include: the strategy for applications security; the network security strategy; the public key infrastructure (PKI) strategy; the role-based access control (RBAC) strategy; and so on. For every major area of the business requirements identified in the contextual architecture, there will be a security strategy (or group of strategies) that supports it.

- *Where* we want to achieve the protection, in terms of location dependency.

The important concepts here are security domains (both logical and physical), domain boundaries and security associations.

- *Who* is involved in security management, in terms of organisational models.

The important concepts are security policy authorities, registration authorities, certification authorities, etc., security organisation and the workflow of security management.

- *When* is the protection relevant, in terms of both points in time and periods of time.

The important concepts are lifetimes and expiry (of keys, certificates, passwords, sessions, etc.), and the use of trusted time for time-stamping and time-sensitive transactions. Also important are time-related performance criteria – how quickly things must happen.

- *Why* the protection is important, in terms of operational risk management.

The important concepts are assets, threats, business impact, vulnerability, risk categorisation, risk mitigation (countermeasures and controls), and cost-benefit analysis.

THE DESIGNER'S VIEW

The designer takes over from the architect. The designer has to interpret the architect's conceptual vision and turn it into a logical structure that can be engineered to create a real building. The architect is an artist and visionary, but the designer is an engineer.

In the world of business computing and data communications, this design process is often called *systems engineering*. It involves the identification and specification of the logical architectural elements of an overall system. This view models the business as a *system*, with *system components* that are themselves *sub-systems*. It shows the major architectural security elements in terms of logical *security services*, and describes the logical flow of control and the relationships between these logical elements. It is therefore also known as the *logical architecture*.

In terms of architectural decomposition down through the layers, the logical security architecture should reflect and represent all of the major security strategies in the conceptual security architecture. At this logical level, everything from

the higher layers is transformed into a series of logical abstractions.

The logical security architecture is concerned with:

- *What*? Specifying the security-related entities and their logical representations, and the relationships between these entities (entity naming, public key certificates, authorisation certificates, messages, etc.).
- *How*? Specifying the logical security services (entity authentication, confidentiality protection, integrity protection, non-repudiation, system assurance, etc.).
- *Where*? Specifying the security domains (logical security domains, physical security domains, security associations).
- *Who*? Specifying the roles and privilege profiles for authorised entities (users, security administrators, auditors, etc.).
- *When*? Specifying the security processing cycle (registration, certification, login, session management, etc.).
- *Why*? Specifying the security policy requirements (high-level security policy, registration authority policy, certification authority policy, physical domain policies, logical domain policies, etc.).

THE BUILDER'S VIEW

The designer of the building hands over the work process to the builder or construction company. The builder is someone who can take the logical descriptions and drawings and turn these into a technology model that can be used to construct the building. It is the builder's job to choose and assemble the physical elements that will make the logical design come to life as a real construction. This view is therefore also referred to as the *physical architecture*.

In our world of business information systems, the designer produces a set of logical abstractions that describe the system to be built. These need to be turned into a physical architecture model that describes the actual technology model and specifies the functional requirements of the various system components. The logical security services are now expressed in terms of the physical security mechanisms and servers that will be used to deliver these services.

In total, the physical security architecture is concerned with:

- *What*? Specifying security-related data structures (tables, messages, pointers, certificates, signatures, etc.)
- *How*? Specifying security mechanisms (encryption, access control, digital signatures, virus scanning, etc.) and the physical servers upon which these mechanisms will be hosted. Capacity, throughput, performance and bandwidth are also specified as attributes of the physical infrastructure.
- *Where*? Specifying security technology infrastructure (physical layout of the hardware, software and communications lines).
- *Who*? Specifying the people dependency in the form of the security user interface (screen formats and user interactions).
- *When*? Specifying the time-dependency in the form of execution control structures (sequences, events, lifetimes and time intervals).
- *Why*? Specifying rules that drive logical decision making within the system (conditions and actions).

THE TRADESMAN'S VIEW

When the builder plans the construction process, s/he needs to assemble a team of experts in each of the building trades that will be needed: the bricklayer, the plasterer, the electrician, the plumber, the carpenter, the steel welder, and so on. Each one of these brings some very specific production skills and some very specific products to the overall construction process.

So it is in the construction of information systems. The builder needs to assemble a series of products from specialist vendors, and a team with the integration skills to join these products together during an implementation of the design.

Each of the integrators is the equivalent of a tradesman, working with specialist products system components that are the equivalent of building materials and components. Some of these trades are hardware-related, some are software-related, and some are service oriented. They work with a series of components that are hardware items, software items, and interface specifications and standards. Hence this layer of the architectural model is also called the *component architecture*.

The component architecture is concerned with:

- *What*? Data field specifications, address specifications and other detailed data specifications.
- *How*? Products and tools (both hardware and software) and standards.
- *Where*? Computer processes, node addresses, and inter-process protocols.
- *Who*? User identities, privileges, and access control lists.

- *When*? Security step timings and sequencing.
- *Why*? Security procedures and steps.

THE FACILITY MANAGER'S VIEW

When the building is finished, those who architected, designed and constructed it move out, but someone has to run the building during its lifetime. We often call such a person the facilities manager. The job of the facilities manager is to deal with the operation of the building and its various services, maintaining it in good working order, and monitoring how well it is performing in meeting the requirements. The framework for doing this is called the *operational architecture*.

In the realm of business information systems the operational architecture is concerned with classical systems operations work. Here we are focusing our attention only on the security-related parts of that work. The operational security architecture is concerned with the following:

- *What*? Maintaining the security of operational business data and information (confidentiality, integrity, authenticity, non-repudiation, availability, auditability, accountability and assurance).
- *How*? Performing specialised security-related operations (user security administration, system security administration, data back-ups, security monitoring, emergency response procedures, etc.).
- *Where*? Maintaining the system integrity and security of all operational platforms and networks (by applying operational security standards and auditing the configuration against these standards).
- *Who*? Providing operational support for the security-related needs of all users (business users, operators, administrators, etc.).
- *When*? Scheduling and executing a timetable of security-related operations.
- *Why*? To maintain operational continuity and security of business data and to avoid operational failures and disruptions.

However, if we refer back to Figure 3, there is another dimension to the operational security architecture – its vertical relationship with the other five layers of the model. This is shown in Table 2, with some examples of the type of operational activity that is implied with regard to each of the other layers.

Table 2: The Operational Security Architecture

At the Contextual Layer	Security policy making, information classification, risk analysis process, business requirements collection and specification, organisational and cultural development, etc.
At the Conceptual Layer	Major programmes for training and awareness, business continuity management, audit and review, process development for registration, authorisation, administration and incident handling, development of standards and procedures, etc.
At the Logical Layer	Management of security services, security of service management, negotiation of inter-operable standards for security services, audit trail monitoring and invocation of actions, etc.
At the Physical Layer	Cryptographic key management, communication of security parameters between parties, synchronisation between parties, ACL maintenance and distribution of ACEs, back-up management (storing, labelling, indexing, etc), virus pattern search maintenance, event log file management and archiving, etc.
At the Component Layer	Products, technology, standards and tools evaluation and selection, project management, implementation management, operation and administration of individual components, etc.

THE INSPECTOR'S VIEW

There is another view of security in business information systems – The Inspector's View – which is concerned with providing assurance that the architecture is complete, consistent, robust and 'fit-for-purpose' in every way. In the realm of information systems security this is the process of 'security auditing' carried out by 'computer auditors'. However, we do not regard this as a separate architectural view. Our approach to audit and assurance is that the architecture model as a whole supports these needs. The existence of such an architecture is one of the ways in which the auditors will establish that security is being applied in a systematic and appropriate way. The framework itself can provide a means by which to structure the audit process. In addition, security audit and review is addressed as one of the major strategic programmes within the operational security architecture associated with the conceptual layer (see Table 1 above).

VERTICAL ANALYSIS OF THE SECURITY ARCHITECTURE

In the above sections we have examined each of the six horizontal layers of abstraction of the architecture model (contextual, conceptual, logical, physical, component and operational). In each of the sections we have also introduced

a series of vertical cuts through each of these horizontal layers, answering the questions:

- *What* are we trying to do at this layer? – The assets to be protected by our security architecture.
- *How* are we trying to do it? – The functions needed to achieve security at this layer.
- *Where* are we doing it? – The locations where we apply our security, relevant to this layer.
- *Who* is involved? – The people and organisational aspects of security at this layer.
- *When* are we doing it? – The time-related aspects of security relevant to this layer.
- *Why* are we doing it? – The motivation for wanting to apply security, expressed in the terms of this layer.

We now summarise these six vertical architectural elements for all six horizontal layers. This gives us a 6 x 6 matrix of cells, which represents the whole model for our enterprise security architecture. If we can address the issues raised by each and every one of these cells, then we will have covered the entire range of questions to be answered, and our security architecture will be complete.

Table 3 shows the matrix of cells representing the overall security architecture framework.

	Assets (What)	Process (How)	Location (Where)	People (Who)	Time (When)	Motivation (Why)
Contextual	Business needs for security	Business processes needing security	Business locations and security	Business security organisation and relationships	Business security time-dependency	Business goals, success factors & operational risks
Conceptual	Business entities, relationships and information	Technical & management security strategies	Security domains and security associations	Security authority organisation and work-flow	Time-related security concepts	Operational risk analysis & risk management
Logical	Security-related data entities & relationships	Security services	Security domain definitions and associations	Roles and privilege profiles	Security processing cycle	Security policies
Physical	Security-related data structures	Security mechanisms	Security technology infrastructure	Security user interface	Control structure execution	Security rules, conditions and actions
Component	Security of data fields & addresses	Security products tools and standards	Processes, nodes, addresses and protocols	User identities, privileges and ACLs	Security step timing and sequencing	Security procedures and steps
Operational	Operational data security	Security operations and administration	Network and platform security	Support for users, operators and administrators	Security operations schedule	Operational continuity