



## **Appendix F2-1**

### Sample Interview (After Fast-Track)

# SABSA® Contextual Security Architecture Development

## Management Interview Guidelines

### Introduction

The main purpose of these interviews is to establish the business drivers for information security in the enterprise, so as to derive the technical security architecture that will support the business goals.

By supplying these guidelines in advance, we hope to maximize the efficiency of the interview itself, and to allow you to prepare your answers. Some answers may be written down in advance on the sheets so as to shorten the interview time required.

The main focus is to see information security as a key *enabler* of business, especially in the use of new technologies to extend business reach and to develop new and improved ways of delivering service. Information security architecture should provide adequate mitigation for the business risks that would otherwise exist, whilst at the same time meeting the wider business requirements for cost, usability, scalability, flexibility, interoperability, and so on.

These interview guidelines cover a series of questions that we would like to discuss with business managers about how information and information systems are expected to support business development, and how managing the various risks associated with this deployment will be the key to providing confidence in these new approaches.

### Validation of the Business Model

We have already identified some of the business needs for information security within HCFA. These are summarized below, and we ask you to comment as appropriate:

- Do you agree?
- Do you disagree?
- Do you have any comments that will qualify these business requirement statements?
- Can you suggest any additional business needs for information security?
- What are the security attributes associated with these business requirements? (see Appendix A)
- What are the risk implications in terms of business impact? (see Appendix B)

In making your comments, please suggest any specific security attributes that are especially relevant, and any specific levels of business impact that might be suffered if these needs cannot be met. You will find a simple and concise explanation of these attributes and impact levels in appendices A and B at the end of this guideline document.

<b>Business Need for Information Security</b>	<b>Agree?</b>	<b>Disagree?</b>	<b>Comments and Suggestions Relevant Security Attributes</b>	<b>Impact level</b>
Protecting the reputation for HCFA				
Maintaining confidence and trust in key relationships:				
Relationship with Congress				
Relationships with individual States				
Relationships with Federal Courts				
Relationships with other Government Agencies				
Relationships with Intermediaries				
Relationships with Beneficiaries				
Relationships with Medical Associations				
Relationships with providers and suppliers of health care services				
Relationships with Institutions				
Relationships with Contractors				
Relationships with other insurers				
Relationships with carriers				
Relationships with taxpayers and the public at large				
Relationships with OIG / GAO				
Relationships with the Press and the media in general				
Internal relationships between management and employees				
Other relationships – please suggest:				
Maintaining operational capabilities and delivery of services				
Supporting the ability to regulate and maintain quality of service across the health care sector				
Providing the ability to resolve disputes				
Maintaining confidence in HCFA such that continued funding is protected				
Protecting business information of the following types:				

<b>Business Need for Information Security</b>	<b>Agree?</b>	<b>Disagree?</b>	<b>Comments and Suggestions Relevant Security Attributes</b>	<b>Impact level</b>
Claims information				
Appeals information				
Patient information				
Other information – please suggest:				
Protecting business processes of the following types:				
Claims processing				
Appeals processing				
Compliance management				
Relationship management				
Other processes – please suggest:				
Protecting intra-office and inter-office communications and information flows, including the following locations:				
Central office				
Regional offices				
Points of service to beneficiaries, both real and virtual				
Government offices and other agencies				
Other locations – please suggest:				
Maintaining timeliness and authorization management with respect to business deadlines				
Hours of business (time of day, day of week, etc)				
Agreed response times for processing claims, appeals, queries, etc.				
Target service times for dealing with on-line beneficiary inquiries				
Annual budget information preparation and presentation for funding support				
Other time-related aspects of information processing that might impact on security requirements – please suggest:				
Supporting the business goals and success factors within Cablevision:				
Operational risk management goals				

Business Need for Information Security	Agree?	Disagree?	Comments and Suggestions Relevant Security Attributes	Impact level
Performance targets				
Cost targets				
Critical success factors for the organization (please specify):				
Other goals and success factors – please suggest:				
Other business needs for information security – please suggest:				

## Further Exploring the Business Model

We would like to discuss with you the following questions:

<b>Qu. 1: The Internet</b>	
How do you see the Internet being developed as a tool for use by HCFA?	
What kinds of applications and usage do you see being developed and rolled out using the Internet over the next few years?	
What risks could HCFA face in doing this?	
What sorts of business impact level would result?	
What are the special information security requirements resulting from these Internet developments?	

<b>Qu. 2: Intranets</b>	
How do you see intranets being developed as a tool for use by HCFA?	
What kinds of applications and usage do you see being developed and rolled out using intranets over the next few years?	
What risks could HCFA face in doing this?	
What sorts of business impact level would result?	
What are the special information security requirements resulting from these intranet developments?	

<b>Qu. 3: Remote Working</b>	
How will 'remote working' be developed in HCFA using on-line information systems?	
What kinds of applications and usage do you see being developed and rolled out using remote working over the next few years?	
What parties will be involved and between which sites and locations will the remote working occur?	
What risks could HCFA face in doing this?	
What sorts of business impact level would result?	
What are the special information security requirements resulting from remote working developments?	

<b>Qu. 4: Mobile Working</b>	
How will 'mobile working' be developed in HCFA using portable computers and possibly portable telephone/modems?	
What kinds of applications and usage do you see being developed and rolled out using mobile working over the next few years?	
What parties will be involved and between which sites and locations will the mobile working occur?	
What risks could HCFA face in doing this?	
What sorts of business impact level would result?	
What are the special information security requirements resulting from mobile working developments?	

<b>Qu. 5: New Ways of Working</b>	
What other new ways of working can you envisage for HCFA based on new information systems and new technologies?	
What specific new technologies or approaches do you think are of potential benefit to HCFA in re-engineering its business processes and ways of working?	
What new risks could HCFA face as the ways of working change and evolve?	
What sorts of business impact level would result?	
What are the special information security requirements resulting from new business practices and new ways of working?	

<b>Qu. 6: Other Suggestions</b>	
By now you will have got the idea of what we are trying to discover through these interviews. Do you have any other suggestions or ideas that you think will be relevant?	

## Appendix A: Security Attributes of Business Information

The following provides an overview of the six main security attributes associated with business information:

- **Integrity:** Assuring the correctness, authenticity and non-repudiability of the source and contents of business-relevant information (static information, traffic information and management information) according to the requirements of the business.
- **Confidentiality:** Preventing the unauthorized disclosure of business information, according to the requirements of the business, and providing assurance that only intended recipients can handle business relevant static, traffic and management information.
- **Availability:** Ensuring that business information systems are ‘up-and-running’ and available for use and that the business information can be accessed by authorized users, according to the requirements of the business. Thus providing assurance of access to, creation of or deletion of business relevant, static, traffic and management data.
- **Accountability:** Maintaining permanent and incontrovertible evidence of the activities performed within business information systems, such that breaches of security can be detected and users can be held responsible for their actions, according to the requirements of the business.
- **Assurance:** Ensuring that the business information systems are designed, built, implemented and operated in such a way as to uphold the security attributes above, according to the requirements of the business, and that auditable evidence is provided to underpin this assurance.
- **Security Management:** Ensuring that the entire environment in which the business information systems are operated has adequate security embedded into the business processes, according to the requirements of the business.

## Appendix B: High-Level Risk Assessment

‘Business impact’ is the term we use to describe how much damage and pain the enterprise will suffer if a particular risk outcome were to crystallise.

For simplicity we measure this level of impact on a three-point scale:

- **HIGH:** **Severe Impact:** The organization suffers a severe set-back to its business goals and stability, perhaps even threatening the future viability of the organization. Personal careers of key managers may be interrupted, and strategic business goals abandoned.
- **MEDIUM:** **Significant Impact:** The organization will survive this event, but there will be significant damage to the business development plans and progress towards the achievement of these. Some managers may find that their careers are damaged, at least in the short to medium term.
- **LOW:** **Minor Impact:** The organization is resilient to this type of event, which is widely regarded as the type of problem that business managers have to deal with almost on an everyday basis.