Appendix **A**

SABSA Business Attributes and Metrics

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
User attributes. These attributes are related to the user's experience of interacting with the business system.			
Accessible	Information to which the user is entitled to gain access should be easily found and accessed by that user.	Soft	Search tree depth necessary to find the information
Accurate	The information provided to users should be accurate within a range that has been preagreed upon as being applicable to the service being delivered.	Hard	Acceptance testing on key data to demonstrate compliance with design rules
Anonymous	For certain specialized types of service, the anonymity of the user should be protected.	Hard Soft	Rigorous proof of system functionality Red team review*
Consistent	The way in which log-in, navigation, and target services are presented to the user should be consistent across different times, locations, and channels of access.	Hard Soft	Conformance with design style guides Red team review

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Current	Information provided to users should be current and kept up to date, within a range that has been preagreed upon as being applicable for the service being delivered.	Hard	Refresh rates at the data source and replication of refreshed data to the destination
Duty-segregated	For certain sensitive tasks, the duties should be segregated so that no user has access to both aspects of the task.	Hard	Functional testing
Educated and aware	The user community should be educated and trained so that they can embrace the security culture There should be sufficient user awareness of security issues so that behavior of users is compliant with security policies.	Soft	Competence surveys
Informed	The user should be kept fully informed about services, operating procedures, operational schedules, planned outages, and so on.	Soft	Focus groups or satisfaction surveys
Motivated	The interaction with the system should add positive motivation to the user to complete the business tasks at hand.	Soft	Focus groups or satisfaction surveys
Protected	The user's information and access privileges should be protected against abuse by other users or by intruders.	Soft	Penetration test. (Could be regarded as "hard," but only if a penetration is achieved. Failure to penetrate does not mean that penetration is impossible.)
Reliable	The services provided to the user should be delivered at a reliable level of quality.	Soft	A definition of "quality" is needed against which to compare.
Responsive	The users obtain a response within a satisfactory period of time that meets their expectations.	Hard	Response time

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Supported	When a user has problems or difficulties in using the system or its services, there should be a means by which the user can receive advice and support so that the problems can be resolved to the satisfaction of the user.	Soft	Focus groups or satisfaction surveys. Independent audit and review against Security Architecture Capability Maturity Model†
Timely	Information is delivered or made accessible to the user at the appropriate time or within the appropriate time period.	Hard	Refresh rates at the data source and replication of refreshed data to the destination
Transparent	Providing full visibility to the user of the logical process but hiding the physical structure of the system (as a url hides the actual physical locations of Web servers).	Soft	Focus groups or satisfaction surveys. Independent audit and review against Security Architecture Capability Maturity Model†
Usable	The system should provide easy-to-use interfaces that can be navigated intuitively by a user of average intelligence and training level (for the given system). The user's experience of these interactions should be at best interesting and at worst neutral.	Soft	Numbers of "clicks" or keystrokes required. Conformance with industry standards, e.g., color palettes. Feedback from focus groups.
Management attributes. This group of attributes is related to the ease and effectiveness with which the business system and its services can be managed.			
Automated	Wherever possible (and depending upon cost/benefit factors) the management and operation of the system should be automated.	Soft	Independent design review

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Change-managed	Changes to the system should be properly managed so that the impact of every change is evaluated and the changes are approved in advance of being implemented.	Soft	Documented change management system, with change management history, evaluated by independent audit
Controlled	The system should at all times remain in the control of its managers. This means that the management will observe the operation and behavior of the system, will make decisions about how to control it based on these observations, and will implement actions to exert that control.	Soft	Independent audit and review against Security Architecture Capability Maturity Model†
Cost-effective	The design, acquisition, implementation, and operation of the system should be achieved at a cost that the business finds acceptable when judged against the benefits derived.	Hard	Individual budgets for the phases of development and for ongoing operation, maintenance and support
Efficient	The system should deliver the target services with optimum efficiency, avoiding wastage of resources.	Hard	A target efficiency ratio based on (Input value)/(Output value)
Maintainable	The system should capable of being maintained in a state of good repair and effective, efficient operation. The actions required to achieve this should feasible within the normal operational conditions of the system.	Soft	Documented execution of a preventive maintenance schedule for both hardware and software, correlated against targets for continuity of service, such as mean time between failures (MTBF)
Measured	The performance of the system should be measured against a variety of desirable performance targets so as to provide feedback information to support the management and control process.	Hard	Documented tracking and reporting of a portfolio of conventional system performance parameters, together with other attributes from this list

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Supportable	The system should be capable of being supported in terms of both the users and the operations staff, so that all types of problems and operational difficulties can be resolved.	Hard	Fault-tracking system providing measurements of MTBF, MTTR (mean time to repair), and maximum time to repair, with targets for each parameter
Operational attributes. These attributes describe the ease and effectiveness with which the business system and its services can be operated.			
Available	The information and services provided by the system should be available according to the requirements specified in the service-level agreement (SLA).	Hard	As specified in the SLA
Continuous	The system should offer "continuous service." The exact definition of this phrase will always be subject to a SLA.	Hard	Percentage up-time correlated versus scheduled and/or unscheduled downtime, or MTBF, or MTTR
Detectable	Important events must be detected and reported.	Hard	Functional testing
Error-free	The system should operate without producing errors.	Hard	Percentage or absolute error rates (per transaction, per batch, per time period, etc.)
Interoperable	The system should interoperate with other similar systems, both immediately and in the future, as intersystem communication becomes increasingly a requirement.	Hard	Specific interoperability requirements
Monitored	The operational performance of the system should be continuously monitored to ensure that other attribute specifications are being met. Any deviations from acceptable limits should be notified to the systems management function.	Soft	Independent audit and review against Security Architecture Capability Maturity Model[†]

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Productive	The system and its services should operate so as to sustain and enhance productivity of the users, with regard to the business processes in which they are engaged.	Hard	User output targets related to specific business activities
Recoverable	The system should be able to be recovered to full operational status after a breakdown or disaster, in accordance with the SLA.	Hard	As specified in the SLA.
Risk management attributes. These attributes describe the business requirements for mitigating operational risk. This group most closely relates to the "security requirements" for protecting the business.			
Access-controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access. Unauthorized access should be prevented.	Hard	Reporting of all unauthorised access attempts, including number of incidents per period, severity, and result (did the access attempt succeed?)
Accountable	All parties having authorized access to the system should be held accountable for their actions.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† with respect to the ability to hold accountable all authorized parties
Assurable	There should be a means to provide assurance that the system is operating as expected and that all of the various controls are correctly implemented and operated.	Hard Soft	Documented standards exist against which to audit Independent audit and review against Security Architecture Capability Maturity Model†

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Assuring honesty	Protecting employees against false accusations of dishonesty or malpractice.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† with respect to the ability to prevent false accusations that are difficult to repudiate
Auditable	The actions of all parties having authorized access to the system, and the complete chain of events and outcomes resulting from these actions, should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail, in accordance with business needs.	Soft	Independent audit and review against Security Architecture Capability Maturity Model†
	The actual configuration of the system should also be capable of being audited so as to compare it with a target configuration that represents the implementation of the security policy that governs the system.	Hard	Documented target configuration exists under change control with a capability to check current configuration against this target
		Soft	Independent audit and review against Security Architecture Capability Maturity Model†
Authenticated	Every party claiming a unique identity (i.e., a claimant) should be subject to a procedure that verifies that the party is indeed the authentic owner of the claimed identity.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† with respect to the ability to authenticate successfully every claim of identity
Authorized	The system should allow only those actions that have been explicitly authorized.	Hard	Reporting of all unauthorized actions, including number of incidents per period, severity, and result (did the action succeed?)

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Authorized (*cont.*)		Soft	Independent audit and review against Security Architecture Capability Maturity Model† with respect to the ability to detect unauthorized actions
Capturing new risks	New risks emerge over time. The system management and operational environment should provide a means to identify and assess new risks (new threats, new impacts, or new vulnerabilities).	Hard	Percentage of vendor-published patches and upgrades actually installed
		Soft	Independent audit and review against Security Architecture Capability Maturity Model† of a documented risk assessment process and a risk assessment history
Confidential	The confidentiality of (corporate) information should be protected in accordance with security policy. Unauthorized disclosure should be prevented.	Hard	Reporting of all disclosure incidents, including number of incidents per period, severity, and type of disclosure
Crime-free	Cyber-crime of all types should be prevented.	Hard	Reporting of all incidents of crime, including number of incidents per period, severity, and type of crime
Flexibly secure	Security can be provided at various levels, according to business need. The system should provide the means to secure information according to these needs, and may need to offer different levels of security for different types of information (according to security classification).	Soft	Independent audit and review against Security Architecture Capability Maturity Model†

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Identified	Each entity that will be granted access to system resources and each object that is itself a system resource should be uniquely identified (named) such that there can never be confusion as to which entity or object is being referenced.	Hard	Proof of uniqueness of naming schemes
Independently secure	The security of the system should not rely upon the security of any other system that is not within the direct span of control of this system.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical security architecture at conceptual, logical, and physical layers
In our sole possession	Information that has value to the business should be in the possession of the business, stored and protected by the system against loss (as in no longer being available) or theft (as in being disclosed to an unauthorised party). This will include information that is regarded as "intellectual property."	Soft	Independent audit and review against Security Architecture Capability Maturity Model†
Integrity-assured	The integrity of information should be protected to provide assurance that it has not suffered unauthorized modification, duplication, or deletion.	Hard	Reporting of all incidents of compromise, including number of incidents per period, severity, and type of compromise
		Soft	Independent audit and review against Security Architecture Capability Maturity Model† with respect to the ability to detect integrity compromise incidents

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Non-repudiable	When one party uses the system to send a message to another party, it should *not* be possible for the first party to falsely deny having sent the message, or to falsely deny its contents.	Hard	Reporting of all incidents of unresolved repudiations, including number of incidents per period, severity, and type of repudiation
		Soft	Independent audit and review against Security Architecture Capability Maturity Model† with respect to the ability to prevent repudiations that cannot be easily resolved
Owned	There should be an entity designated as "owner" of every system. This owner is the policy maker for all aspects of risk management with respect to the system, and exerts the ultimate authority for controlling the system.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of the ownership arrangements and of the management processes by which owners should fulfil their responsibilities, and of their diligence in so doing
Private	The privacy of (personal) information should be protected in accordance with relevant privacy or "data protection" legislation, so as to meet the reasonable expectation of citizens for privacy. Unauthorized disclosure should be prevented.	Hard	Reporting of all disclosure incidents, including number of incidents per period, severity, and type of disclosure
Trustworthy	The system should be able to be trusted to behave in the ways specified in its functional specification and should protect against a wide range of potential abuses.	Soft	Focus groups or satisfaction surveys researching the question "Do you trust the service?"

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Legal and regulatory attributes. This group of attributes describes the business requirements for mitigating operational risks that have a specific legal or regulatory connection.			
Admissible	The system should provide forensic records (audit trails and so on) that will be deemed to be "admissible" in a court of law, should that evidence ever need to be presented in support of a criminal prosecution or a civil litigation.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† by computer forensics expert
Compliant	The system should comply with all applicable regulations, laws, contracts, policies, and mandatory standards, both internal and external.	Soft	Independent compliance audit with respect to the inventories of regulations, laws, policies, etc.
Enforceable	The system should be designed, implemented and operated such that all applicable contracts, policies, regulations, and laws can be enforced by the system.	Soft	Independent review of: (1) inventory of contracts, policies, regulations and laws for completeness, and (2) enforceability of contracts, policies, laws, and regulations on the inventory
Insurable	The system should be risk-managed to enable an insurer to offer reasonable commercial terms for insurance against a standard range of insurable risks	Hard	Verify against insurance quotations
Legal	The system should be designed, implemented, and operated in accordance with the requirements of any applicable legislation. Examples include data protection laws, laws controlling the use of cryptographic technology, laws controlling insider dealing on the stock market, and laws governing information that is considered racist, seditious, or pornographic.	Soft	Independent audit and review against Security Architecture Capability Maturity Model.† Verification of the inventory of applicable laws to check for completeness and suitability

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Liability-managed	The system services should be designed, implemented and operated so as to manage the liability of the organization with regard to errors, fraud, malfunction, and so on. In particular, the responsibilities and liabilities of each party should be clearly defined.	Soft	Independent legal expert review of all applicable contracts, SLAs, etc.
Regulated	The system should be designed, implemented, and operated in accordance with the requirements of any applicable regulations. These may be general (such as safety regulations) or industry-specific (such as banking regulations).	Soft	Independent audit and review against Security Architecture Capability Maturity Model†. Verification of the inventory of applicable regulations to check for completeness and suitability
Resolvable	The system should be designed, implemented and operated in such a way that disputes can be resolved with reasonable ease and without undue impact on time, cost, or other valuable resources.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† by legal expert
Time-bound	Meeting requirements for maximum or minimum periods of time, for example, a minimum period for records retention or a maximum period within which something must be completed.	Hard	Independent functional design review against specified functional requirements
Technical strategy attributes. This group of attributes describes the needs for fitting into an overall technology strategy.			
Architecturally open	The system architecture should, wherever possible, not be locked into specific vendor interface standards and should allow flexibility in the choice of vendors and products, both initially and in the future.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
COTS/GOTS compliant	Wherever possible, the system should utilize commercial off-the-shelf or government off-the-shelf components, as appropriate.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Extendable	The system should be capable of being extended to incorporate new functional modules as required by the business.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical & physical)
Flexible & Adaptable	The system should be flexible and adaptable to meet new business requirements as they emerge.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Future-proof	The system architecture should be designed as much as possible to accommodate future changes in both business requirements and technical solutions.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Legacy-sensitive	A new system should be able to work with any legacy systems or databases with which it needs to interoperate or integrate.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Migrateable	There should be a feasible, manageable migration path, acceptable to the business users, that moves from an old system to a new one, or from one released version to the next.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Multisourced	Critical system components should be obtainable from more than one source, to protect against the risk of the single source of supply and support being withdrawn.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture at the component level
Scaleable	The system should be scaleable to the size of user community, data storage requirements, processing throughput, and so on that might emerge over the lifetime of the system.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Simple	The system should be as simple as possible, since complexity only adds further risk.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Standards compliant	The system should be designed, implemented and operated to comply with appropriate technical and operational standards.	Soft	Independent audit and review of: (1) the inventory of standards to check for completeness and appropriateness, and (2) compliance with standards on the inventory
Traceable	The development and implementation of system components should be documented so as to provide complete two-way traceability. That is, every implemented component should be justifiable by tracing back to the business requirements that led to its inclusion in the system, and it should be possible to review every business requirement and demonstrate which of the implemented system components are there to meet this requirement.	Soft	Independent expert review of documented traceability matrices and trees

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Upgradeable	The system should be capable of being upgraded with ease to incorporate new releases of hardware and software.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, and physical)
Business strategy attributes. This group of attributes describes the needs for fitting into an overall business strategy.			
Brand enhancing	The system should help to establish, build, and support the brand of the products or services based upon this system.	Soft	Market surveys
Business-enabled	Enabling the business and fulfilling business objectives should be the primary driver for the system design.	Soft	Business management focus group
Competent	The system should protect the reputation of the organization as being competent in its industry sector	Soft	Independent audit, or focus groups, or satisfaction surveys
Confident	The system should behave in such a way as to safeguard confidence placed in the organization by customers, suppliers, shareholders, regulators, financiers, the marketplace, and the general public.	Soft	Independent audit, or focus groups, or satisfaction surveys
Credible	The system should behave in such a way as to safeguard the credibility of the organization.	Soft	Independent audit, or focus groups, or satisfaction surveys
Culture-sensitive	The system should be designed, built, and operated with due care and attention to cultural issues relating to those who will experience the system in any way. These issues include such	Soft	Independent audit and review of (1) the inventory of requirements in this area to check for completeness and

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Culture-sensitive (*cont.*)	matters as religion, gender, race, nationality, language, dress code, social customs, ethics, politics, and the environment. The objective should be to avoid or minimize offence or distress caused to others.		appropriateness, and (2) compliance of system functionality with this set of requirements
Enabling time-to-market	The system architecture and design should allow new business initiatives to be delivered to the market with minimum delay.	Soft	Business management focus group
Governable	The system should enable the owners and executive managers of the organization to control the business and to discharge their responsibilities for governance.	Soft	Senior management focus group. Independent audit and review against Security Architecture Capability Maturity Model† for governance
Providing good stewardship and custody	Protecting other parties with whom we do business from abuse, loss of business, or personal information of value to those parties through inadequate stewardship on our part.	Soft	Independent audit, or focus groups, or satisfaction surveys
Providing investment reuse	As much as possible, the system should be designed to reuse previous investments and to ensure that new investments are reusable in the future.	Soft	Independent audit and review against Security Architecture Capability Maturity Model† of technical architecture (conceptual, logical, physical, and component)
Providing return on investment	The system should provide a return of value to the business to justify the investment made in creating and operating the system.	Hard Soft	Financial returns and RoI indices selected in consultation with the Chief Financial Officer Qualitative value propositions tested by opinion surveys at senior management and boardroom level

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Reputable	The system should behave in such a way as to safeguard the business reputation of the organization.	Soft	Independent audit, or focus groups, or satisfaction surveys
		Hard	Correlation of the stock value of the organization versus publicity of system event history

*A red team review is an objective appraisal by an independent team of experts who have been briefed to think either like the user or like an opponent/attacker, whichever is appropriate to the objectives of the review.

†The type Architectural Capability Maturity Model referred to is based upon the ideas of capability maturity models.