

**Work Program – Internet Banking**

**1 OVERVIEW**

**1.1 Introduction**

[Insert background information on the Internet Banking project]

**1.2 Organisational structure**

[Insert an organisational structure,]

**1.3 Key systems**

[Expand on the systems information and provide a systems diagram]

**1.3.1 System overview – current systems**

System	Function	Provider/Name	Comment
--------	----------	---------------	---------

**1.3.2 Message flow through systems**

Insert message flow through all systems.

**1.3.3 Access control matrix of personnel (by job description) to system (optional)**

## 2.1 Policy

**Key risk** There is a risk that standards, procedures and guidelines may not provide sufficient guidance to manage risk of internet banking applications if the internet security policy is not defined, assessed and agreed by senior management.

### Key controls

#### 2.1.1 Control objective:

*Internet Banking security policies and standards exist, are regularly reviewed, and are formally ratified by senior management*

Control Applied	Work Performed	Observations
An Internet Banking Security policy exists and is approved by Senior Management		
The Internet Banking Security Policy(s) is kept current in line with EU and national government bills, laws and guidelines.		
The Internet Banking Security Policy(s) is regularly reviewed for adequacy based upon the evolving technology and changing user/customer requirements		
The Internet Banking Security Policy(s) include or refer to existing Service Access policies and Firewall security policies.		
Procedures for security incident alert and escalation have been clearly defined, documented and implemented.		
The updates and changes to the Internet Banking Security Policy(s) are clearly defined and agreed by senior management.		

#### 2.1.2 Control objective:

*Personnel related Information Systems (IS) security policies and standards have been defined and documented*

Control Applied	Work Performed	Observations
IS security awareness programs have been implemented		
IS security policies and standards address access violation attempts		
Employee termination and transfer procedures have been implemented and documented		

## 2.2 Operational Controls - Access

With an internet banking system using distributed systems, many points of access are available that need to be controlled and monitored. The points of access include:

1. User machine and front end application
2. Internet infrastructure
3. Access router and external firewall
4. Web and application server
5. Local area network infrastructure
6. Mainframe

### Key controls

**2.2.1** *For each internet banking infrastructure component, adequate user identification procedures have been implemented, access controls exist on application data, and documented audit trails are maintained*

Control Applied	Work Performed	Observations
Effective security mechanisms are in place to prevent unauthorised access to other accounts.		
Access control mechanisms are employed to control access both in and out of the Internal network.		
Effective security mechanisms are in place to prevent unauthorised access to each functional infrastructure component.		
Access control mechanisms are employed to control access of unauthorized persons to the transaction processing functions of application programs.		
Adequate logging, reporting and surveillance facilities exist within the system		
Adequate log administration and monitoring procedures have been implemented		
Automated tools are used to highlight log entries that suggest a penetration attempt.		
A network time protocol is used to synchronise the server system clocks to enable accurate and consistent time stamping of events.		
Both proactive and detective monitoring are performed to highlight attempted or successful security breaches of the system.		
Logs are reviewed on a daily basis for successful and unsuccessful attempts to penetrate security.		
Multiple unsuccessful login attempts are logged and called to the attention of the system administrator for resolution.		
Audit trail recording application activity have		

Control Applied	Work Performed	Observations
been implemented and secured.		
Adequate access restrictions over software logs and audit trails have been implemented.		

**2.2.2 Control objective:**

***Helpdesk and registration operations are operated to a consistent standard and do not allow direct access to customer records.***

Control Applied	Work Performed	Observations
Helpdesk operational procedures exist and include FAQ's, scripts, and procedures to access to a problem database.		
The procedures exist for helpdesk request escalation and helpdesk staff are fully trained on the proper procedures.		
The helpdesk operational procedures are kept current and updated to reflect core application developments, updates or changes. Helpdesk staff are notified of any impending changes.		
The Helpdesk is split into three lines of support: <ul style="list-style-type: none"> <li>• Front line support (tackle all queries)</li> <li>• Technical issues which the front line are unable to answer are passed on to Technical support.</li> <li>• Customer information changes are noted by Front line support and passed to Back office support for update.</li> </ul> Staff are supplied with procedures and training material.		
The helpdesk operational procedures are kept current and updated to reflect core application developments, updates or changes. Helpdesk staff are notified of any impending changes.		
The registration procedures have been clearly defined, documented, and implemented.		
Registration process only permits valid customers to register as Internet Banking customers. Member authentication details (e.g. membership numbers, passcodes, digital certificates, tokens, ...) are issued securely to the customer.		

**2.2.3 Control objective:**

***There exist appropriate controls to prevent unauthorised access to Internet banking operations facilities, commands, programs and data.***

Control Applied	Work Performed	Observations
Organisation structure and management permits segregation of duty		
Effective security mechanisms are in place to prevent unauthorised access to customer data. Password authentication exists and ensures that:		

<b>Control Applied</b>	<b>Work Performed</b>	<b>Observations</b>
<ul style="list-style-type: none"> <li>• access is only permitted by use of a valid logon ID and password combination (User IDs should be unique and passwords should be specific to one ID)</li> <li>• logon IDs are automatically disabled after a prescribed number of logon failures or a set period of inactivity</li> <li>• logon IDs and passwords are revoked when employees leave or relocate within the organisation</li> </ul>		
3 <sup>rd</sup> Party businesses related to Internet Banking have restricted access to relevant and necessary customer data.		
Appropriate maintenance of Internet banking hardware and software is undertaken		
Documentation exists to support all Internet banking systems, applications and operational procedures		
Change control procedures have been defined, documented and implemented.		
Recovery from operational failures is subject to documented procedures		
Physical access to critical Internet banking system components is properly secured, controlled and restricted to authorised personnel only		
Physical and environmental controls to protect the equipment have been implemented, including protection against risks caused by natural disasters (e.g. fire, power losses, etc.)		

**2.2.4 Control objective:**  
*The role and responsibilities of the Information Systems Administration (ISA) function have been defined and documented*

<b>Control Applied</b>	<b>Work Performed</b>	<b>Observations</b>
Responsibility for the security administration of Internet Banking Services has been assigned.		
Detailed job roles have been defined, which clearly state the security administration tasks to be performed.		
Adequate segregation of duties exists within the ISA function		
ISA staff are adequately trained.		
Detailed procedures and guidelines for the ISA function have been defined and documented.		
Access violation attempts are monitored and reported by IS security.		

**2.2.5 Control objective:**

***Internet Banking Services are delivered through a suitable firewall architecture.***

Control Applied	Work Performed	Observations
A firewall architecture has been designed and implemented in order to support Internet Banking Services.		
Internet Banking and other e-services are delivered through a dedicated firewall architecture (i.e. not shared with general external Internet access for the organisation)		

**2.2.6 Control objective:**

***Firewalls have been tested to ensure that no unknown security vulnerabilities exist.***

Control Applied	Work Performed	Observations
A penetration test has been carried out and any weakness outlined in the penetration test report has been evaluated and acted on.		
The adequacy of the penetration test can be verified.		
Monitoring of firewall should alert operators of penetration test underway		
Automated tools are used to highlight log entries that suggest a penetration attempt.		
All ports have been listed with the application requirements for each port		

**2.2.7 Control objective:**

***Automatic mechanisms and manual reporting procedures identify unauthorised access through firewalls***

Control Applied	Work Performed	Observations
Adequate logging, reporting and surveillance facilities exist within the firewall software		
The firewall contains a mechanism for logging traffic and suspicious activity, and employs a mechanism so that critical log entries are highlighted and brought to the attention of the system administrator.		
Both proactive and detective monitoring are performed to highlight attempted or successful security breaches of the system.		
Logging is performed by the firewall system on inbound and outbound services.		
Automated tools are used to highlight log entries that suggest a penetration attempt.		
Adequate log administration and monitoring procedures have been implemented		
Adequate access restrictions over software logs and audit trails have been implemented		
Firewall logs are stored off the firewall system.		

Control Applied	Work Performed	Observations
Logs are reviewed on a daily basis for successful and unsuccessful attempts to penetrate security.		
Multiple unsuccessful login attempts are logged and called to the attention of the system administrator for resolution.		
Audit trail recording application activity have been implemented and secured.		
A network time protocol is used to synchronise the firewall system clocks to enable accurate and consistent time stamping of events.		
Adequate access restrictions over software logs and audit trails have been implemented.		

**2.2.8 Control objective:**

***Firewalls are managed in a timely manner to protect against unauthorised access or attack***

Control Applied	Work Performed	Observations
Adequate firewall change control procedures are defined, documented and agreed by senior management.		
Change control procedures are managed and monitored.		
Management approval is needed before firewall applications can be altered or upgraded.		
Management approval is needed before router or firewall system operating systems can be altered or upgraded.		
Management approval is needed before firewall access control rules can be added/deleted or modified (including routers).		
Changes to firewall applications are tested before migration to the production firewall system, and impact assessment is performed to ensure that new vulnerabilities are not exposed		
Update notification is made when firewalls need update from vendor (Sun) and from security advisory bodies (such as CERT, bugtrak).		
The firewall application system is updated with patches and other bug fixes in a timely fashion.		
Physical access to firewall system components is properly secured, controlled and restricted to authorised personnel only		
Emergency access control procedures for firewall support and administration have been defined.		

**2.2.9 Control objective:**

***Application development is segregated from live and test environments***

Control Applied	Work Performed	Observations
Separate testing and development environment exist and applications can be fully implemented		

<b>Control Applied</b>	<b>Work Performed</b>	<b>Observations</b>
and tested on a separate test environment.		
Formal sign-off procedures are documented for the movement of new applications, updates, patches and fixes from development through testing to production.		
Formal sign-off procedures are adhered to.		
A testing strategy for the release of Internet Banking has been defined and documented.		
An adequate organisational and management structure has been put in place for testing to ensure segregation of duties with respect to development and testing.		
A formal mechanism for system scope changes has been defined		
The testing procedures are fully documented and cover unit testing, system testing, stress testing and regression testing.		
Emergency change procedures have been defined, documented and are followed.		
Test plans describe the required testing environments and resource requirements for each cycle of testing		
Performance monitoring, and tuning forms part of the testing process		

**2.2.10 Control objective:**

*Network security design and administration of security functions allow for appropriate controls*

<b>Control Applied</b>	<b>Work Performed</b>	<b>Observations</b>
Network access is appropriately controlled.		
Network has sufficient number of perimeters.		
Separate internal and external Domain Name System (DNS) servers are utilized to “mask” internal host names from the Internet.		
All internal IP addresses are hidden from internet user through techniques such as Network Address Translation (NAT)		
Access control mechanisms are employed to control access both in and out of the Internal network.		
Router configurations are regularly evaluated to determine if any authorized or unauthorized changes were made.		
Adequate logging, reporting and surveillance facilities exist within the system		
Automated tools (e.g. SNMP) are used to highlight log entries that suggest anomalous activity.		
Adequate log administration and monitoring procedures have been implemented		

Control Applied	Work Performed	Observations
Both proactive and detective monitoring are performed to highlight attempted or successful security breaches of the system.		
Router configurations are evaluated daily to determine if any authorised or unauthorised changes were made.		
Logs are reviewed on a daily basis for successful and unsuccessful attempts to penetrate security.		
Audit trail recording application activity have been implemented and secured.		
Adequate access restrictions over software logs and audit trails have been implemented		
Physical access to network system components, such as routers, is properly secured, controlled and restricted to authorised personnel only		

**2.2.11 Control objective:**

*Access routers limit access between critical systems components (e.g. Firewalls, backend systems)*

Control Applied	Work Performed	Observations
Choke routers are used to filter ICMP and only required TCP/UDP ports		
Routers are logically secured and passwords are controlled		
Routers directly reachable via the Internet do not accept routing updates from the Internet (e.g., RIP updates, ICMP redirects, etc.)		
Intranet routers are configured to ensure communication between Internet Banking systems within the corporate LAN is restricted to the necessary systems.		

**2.2.12 Control objective:**

*Web servers are hardened to protect against Internet attack.*

Control Applied	Work Performed	Observations
Web servers only run required processes		
Web server operating systems should be hardened – no unnecessary daemons. Enhanced security is enabled.		

**2.2.13 Control objective:**

*Network operators manage systems in a secure manner*

Control Applied	Work Performed	Observations
Network maintenance procedures are clearly defined and documented		
Staff have adequate training on servers and gateways.		

**2.2.14 Control objective:**

***Core Internet Banking Systems are managed to protect against unauthorised access***

Control Applied	Work Performed	Observations
Access Control Lists (ACLs) are used and a restricted list of authorised users is maintained.		
The core systems configurations are clearly defined documented.		
Adequate controls are applied to ensure the integrity and security of transactions between the core systems and the mainframe.		
Adequate segregation of duties exists between operational personnel.		
Physical access to core systems or back end system components is properly secured, controlled and restricted to authorised personnel only		
Adequate logging, reporting and surveillance facilities exist within the core systems system.		
Adequate log administration and monitoring procedures have been implemented.		
Audit trail recording core systems activity have been implemented and secured.		
Adequate access restrictions over software logs and audit trails have been implemented.		

**2.2.15 Access to and definition of data held within the Database Management System (DBMS) is adequately controlled**

Control Applied	Work Performed	Observations
Controls over DBMS resources are adequately documented and implemented.		
Access controls to intermediate data are restricted to systems administrators and application users only.		
Sensitive client data (PINs) stored within the DBMS is encrypted.		

**2.2.16 Control objective:**

***Application security design and administration of security functions allow for appropriate controls***

Control Applied	Work Performed	Observations
Password authentication exists and ensures that: <ul style="list-style-type: none"> <li>• access is only permitted by use of a valid logon ID and password combination (User IDs should be unique and passwords should be specific to one ID)</li> <li>• logon IDs are automatically disabled after a prescribed number of logon failures or a set period of inactivity</li> <li>• logon IDs and passwords are revoked when users close accounts.</li> </ul>		

Control Applied	Work Performed	Observations
<ul style="list-style-type: none"> <li>• logon IDs and passwords are temporarily disabled when employees are on leave of absence</li> <li>• simultaneous use of the same user ID at more than one workstation is prohibited</li> <li>• access is restricted by time of day</li> <li>• menu selections displayed are restricted based upon the access privileges defined by the user ID</li> </ul>		
<p>Terminal authentication and security procedures include for system administrator or other privileged access accounts :</p> <ul style="list-style-type: none"> <li>• automatic lock out after a prescribed number of logon failures</li> <li>• automatic log off of terminals after a set period of inactivity</li> <li>• location in restricted access areas</li> </ul>		
<p>User access rights are restricted to those processing functions and data files required for the users normal duties.</p>		
<p>Changes to user access rights are:</p> <ul style="list-style-type: none"> <li>• based only on written authorization, which is retained as an audit trail, and matched against reported changes to access rights</li> <li>• automatically reported and reviewed by management.</li> </ul>		
<p>Password confidentiality is controlled, in that individual passwords are:</p> <ul style="list-style-type: none"> <li>• required by the access control software to be changed at regular intervals</li> <li>• changed by the users when required or on demand</li> <li>• required to be of a minimum length (at least 6 characters) and composition designed to prevent guessing</li> <li>• checked by the system and rejected if they are of an obvious or common nature or the same as those used previously by the same user</li> <li>• not displayed on the terminal screen or written on or near the terminal</li> <li>• not printed onto hard copy logs or reports in an unencrypted format</li> <li>• not disclosed to the security administration function</li> <li>• protected and/or encrypted in the password files/tables</li> </ul>		

## 2.3 Operational Controls - Input

### 2.3.1 Control objective:

*Application has input validation techniques to ensure that information to be processed has correct attributes*

Control Applied	Work Performed	Observations
Application checks data validity before sending message for processing.		
Front end application checks for correct characters, decimal places and number ranges.		

### 2.3.2 Control objective:

*Adequate user identification procedures have been implemented and documented*

Control Applied	Work Performed	Observations
User identification techniques meet business requirements.		
Adequate certification techniques are in place to verify user identity.		
User authentication mechanisms prevent unauthorised access and change to records.		
Controls are in place to identify possible unauthorised users.		

### 2.3.3 Control objective:

*Interface from application to standing data and mainframe data is completed accurately, completely and entered only once.*

Control Applied	Work Performed	Observations
Adequate controls exist to monitor and maintain the integrity of the DBMS		
Intermediate database schema is documented and matches data definition on mainframe. (Users are viewing same data as on mainframe account).		
Controls over the use of sensitive DBMS functions are documented and implemented		
Distributed DBMS components are subject to adequate access and integrity controls		

### 2.3.4 Control objective:

*Application design and administration of data input transactions allow for appropriate controls*

Control Applied	Work Performed	Observations
Transactions are subjected to programmed edit/validation checks which include: <ul style="list-style-type: none"><li>• data directly validated against specified files or tables</li><li>• key fields tested for blanks, alphas, values within a specified range, missing data elements, programmed check digits and appropriate justification</li></ul>		
Exception reports are produced listing large or unusual items, which are then individually compared to input documents.		

Control Applied	Work Performed	Observations
<p>Exception reports are produced listing unmatched items, which are subsequently followed-up.</p> <p>Changes to user-defined system parameters are automatically reported and checked by an independent official.</p> <p>Overrides of system warnings by the user are automatically reported for independent approval.</p>		

## 2.4 Operational Controls – Rejected Items

### 2.4.1 Control objective:

*Application has facility to ensure that user is informed that a transaction has not been processed.*

Control Applied	Work Performed	Observations
<p>Error checking is enabled at stage of the information flow and errors are returned to client application to ensure that notification of incomplete transaction is recorded.</p>		
<p>Can users cancel a transaction that has been accepted and pending a batch update.</p>		

### 2.4.2 Control objective:

*Any transaction rejected after acceptance by input validation and rejected for processing is isolated, analysed and corrected.*

Control Applied	Work Performed	Observations
<p>Transaction alerts are acted on to ensure that rejected items are isolated analysed and corrected.</p>		
<p>Data on rejected transactions is analysed and information fed back to development to enable any application errors to be corrected.</p>		

### 2.4.3 Control objective:

*Supports processes are in place to monitor and correct rejected items.*

Control Applied	Work Performed	Observations
<p>A support function is in place to monitor and correct rejected items.</p>		
<p>The support function is managed to ensure that all items accurately processed and logged.</p>		

**2.5 Operational Controls - Processing**

**2.5.1 Control objective:**

*Formal testing procedures ensure that applications are fully tested before they are released into the production environment.*

Control Applied	Work Performed	Observations
An adequate organisational and management structure has been put in place for testing.		
A testing strategy has been defined, documented and is followed.		
A formal mechanism for system scope changes has been defined.		
The testing procedures are fully documented and cover unit testing, system testing, and regression testing.		
Formal migration procedures have been defined, documented and are followed.		
Change control procedures have been defined, documented and are followed.		
Emergency change procedures have been defined, documented and are followed.		
Test plans exist and are comprehensive		
Test plans describe the required testing environments and resource requirements for each cycle of testing		
Performance monitoring and tuning forms part of the testing process.		
Testing coverage is comprehensive.		
Test plans reflect the implementation strategy.		
Acceptance testing criteria are measurable.		

**2.5.2 Control objective:**

*Version controls ensure that changes are applied to the correct releases and versions of software*

Control Applied	Work Performed	Observations
A version number of each release of client software (HTML page or Java applet) is recorded.		
Version controls ensure that changes are applied to the correct releases and versions of software		
Each version of software is formally approved for release		

**2.5.3 Control objective:**

*Application provides integrity of data from user entry to mainframe update*

Control Applied	Work Performed	Observations
Transactions are completed in a timely manner.		

Control Applied	Work Performed	Observations
Data integrity is checked when transferred from front-end systems to back end systems in a gateway.		
Security measures have been defined and implemented to protect the integrity of the application data.		
Application checks exist to ensure the server has not been spoofed.		

**2.5.4 Control objective:**

***Encryption keys are managed to ensure accurate processing and secure operation of system***

Control Applied	Work Performed	Observations
Keys used for authentication or encryption are adequately managed		
No one can know the total value in clear of a key		
The availability of the keys is guaranteed in every situation		
Keys are stored in a physically secured environment. In other environments keys are not stored in clear.		
Only users and specifically authorised programs by the security administrator have access to use of the keys and encryption functions.		
Critical encryption keys will only reside in physically secure hardware.		
Segregation of duties has been applied to encryption and authentication keys.		
Access to public keys has been restricted to duly authorised users and process. Data processing security has lists of authorised users and processes.		
Exchange of keys is subject to adequate controls		
Procedures for the generation of keys used for authentication or encryption ensure that the security of keys is maintained at all times		
Appropriate administration procedures and policies for key management, where appropriate, are adequate		

**2.5.5 Control objective:**

***PIN/Password controls are appropriately controlled***

Control Applied	Work Performed	Observations
PIN/Password life cycle is defined and enforced through policies and procedures to ensure secure generation, distribution, storage, management, and deletion. ( SLB as a phone banking service may not already have in place a PIN/Password printing and distribution service)		

Control Applied	Work Performed	Observations
Appropriate controls are in place to ensure PIN/Password storage databases are adequately secured and managed		

**2.5.6 Control objective:**  
*The internet access, web server, firewall and core Internet Banking system performance is monitored to ensure there is adequate capacity for Internet Banking transactions*

Control Applied	Work Performed	Observations
Performance statistics are collected for all Internet banking infrastructure components		
Procedures have been defined for regular monitoring the core Internet Banking systems performance to ensure there is adequate capacity for Internet banking transactions		

**2.5.7 Control objective:**  
*Application design and administration of processing transactions allow for appropriate controls*

Control Applied	Work Performed	Observations
Restart and recovery procedures ensure that transactions are not lost as a result of processing interruptions.		
Erroneous or unauthorized system generated transactions are reported for follow-up.		
Reasonableness checks are applied to system generated data; transactions failing checks are reported for review and follow-up		
The validity of the account number is checked through system validation and edit applications.		
Requests that do not have a valid account number are rejected and then investigated with the customer.		
Payments are only accepted for processing if the payment request indicates that it contains a valid account number.		

**2.6 Processing and Stability - Service Management**

**2.6.1 Control objective:**  
*Problem and Incident Management*

Control Applied	Work Performed	Observations
Formal problem management procedures are in place		
Formal crisis management procedures are in place		
Roles and responsibilities for problem and incident management and documented		
Escalation procedures are clearly communicated		

<b>Control Applied</b>	<b>Work Performed</b>	<b>Observations</b>
Recovery of functionality is prioritised and time objectives applied		
Post incident reviews are carried out and reports made to senior management		
Procedures are reviewed periodically by staff and management. Updates to procedure are effectively communicated with training carried out where required. (Version control on docs)		

**2.6.2 Control objective:  
New Systems Acceptance**

<b>Control Applied</b>	<b>Work Performed</b>	<b>Observations</b>
Test plans cover testing of application in isolation and testing all interfaces		
Testing covers all the business objectives initially agreed for the system		
Test results are logged and tests have been successful		
Formal sign-off documents have been signed by senior management (IT & Business)		