X-Bank Project Risk Assessment
Technical Risk
Version 1.0

Version	Date	Contents	Author	Distributed to
Test Site 0.1	XX	First draft: areas of risk defined, risk types defined, document controls in place	AT Shuldiner (Risk Manager)	T Friedman (Project Manager), B van den Brink (Lead Developer)
Test Site 0.2 (live)	XX	Project description, existing controls documented (signed draft)	AT Shuldiner (Risk Manager)	T Friedman (Project Manager), AJ van Rooi (Corporate Audit)
Commercial Pilot 0.3	XX	50% of risk areas completed	AT Shuldiner (Risk Manager)	T Friedman (Project Manager), M Boerma (Security Consultant), F Meerman (Lead Network Architect)
Commercial Pilot 0.4 (live)	XX	75% of risk areas completed; executive summary, risk acceptance responsibilities assigned (signed draft)	AT Shuldiner (Risk Manager)	T Friedman (Project Manager), J Sosa (Chief Technology Officer)
Commercial Launch 1.0 (live)	XX	90% of risk areas completed (signed draft, filed with Risk Management Department)	R van Loon (Risk Manager)	T Friedman (Project Manager), J Sosa (Chief Technology Officer), Corporate Risk Management Department (file copy)
…				

This document is of a highly sensitive nature and should be distributed on a need-to-know basis only. Under no circumstances is this document to be distributed via insecure electronic means (e.g., unencrypted email). *All instances of distribution must be cleared with and reported to the project Security Manager.*

Dr. AT Shuldiner, Basel Consulting
alec@baselconsulting.com

Table of Contents

Dr. AT Shuldiner, Basel Consulting
alec@baselconsulting.com

Introduction

This document is a statement of "technical" risks faced by the X-Bank Online Transaction Project operating in a commercial environment. Technical risks are defined as those risks that arise from the operation of the X-Bank application, its administrative tools, its hosting environment, and any networked services. Technical risks do *not* include risks generated by the activity of registered users on the X-Bank website, whether fraudulent or otherwise: these are covered in the operational risk assessment. Risks are grouped into the following 10 categories derived from the British Standard: "Code of practice for information security management" (numbers refer to BS 7799-1:2000), plus five additional categories of particular concern to the X-Bank project, as follows:

Exhibit 1: Risk Assessment: Areas of Technical Risk for Initial Commercial Launch

Area of Risk	Key Questions for *Initial Commercial Launch*
BS3-Information Security Policy	Is there a policy in place that governs the management of information security and associated risks? Has responsibility for maintenance of that policy been assigned?
BS4-Organizational Security	Are information security and associated risks addressed within a fixed management framework? Are those managerial resources sufficient and clearly designated? Is this area given an appropriate degree of attention by top management? Does X-Bank have access to suitable sources of security expertise?
BS5-Asset Classification and Control	Does the project maintain an inventory of the major IT-related assets it owns, including servers, software, and data? Have all of those assets been given an appropriate security classification? Are those assets assigned to specific owners and have those owners taken the necessary steps to maintain and protect those assets?
BS6-Personnel Security	Are X-Bank employees appropriately screened given their access to sensitive assets? Do they understand relevant security policies and how to conform to them, including reporting requirements? Do X-Bank job contracts contain appropriate safeguards to protect X-Bank intellectual property?
BS7-Physical and Environmental Security	Are the X-Bank business premises protected against unauthorized access? Are they reasonably protected against environmental risks such as fire, water damage, electrical damage, and overheating? Is sensitive IT equipment and software protected by suitable additional security measures? Do X-Bank employees obey a "clear desk" policy? Is equipment correctly maintained? Are appropriate measures in place to ensure the security of assets taken offsite (e.g., laptops and from-home connections)? Is stored data safe from misappropriation?
BS8-Communications and Operations Management	Have proper processes been defined and implemented to govern incident handling, change management, and other sensitive operations? Are duties appropriately segregated? Are these operations auditable? Are development, test, and production facilities properly insulated from one another? Has the chance of system failure been minimized by proper capacity planning and good housekeeping practices (including up-to-date protection against malicious software and reliable backup procedures)? Are those individuals selected to fill the various operating roles qualified to do so?

Dr. AT Shuldiner, Basel Consulting
alec@baselconsulting.com

Area of Risk	Key Questions for *Initial Commercial Launch*
BS9-Access Control (i.e., Logical Security)	Are proper logical security measures in place to protect the X-Bank intranet and administrative tools? Are users of the intranet and of these tools properly educated in the use of those security measures? Do X-Bank employees obey a "clear screen" policy? Is remote access to these tools sufficiently secure?
BS10-System Development and Maintenance	Is existing system functionality sufficiently documented? Is a process in place for incremental documentation of further development? Does the release management process and associated operational processes provide sufficient version control for the X-Bank application? Is the development environment secure? Is the test environment secure?
BS11-Business Continuity Management	Are the possible consequences of disaster sufficiently well understood? Do plans exist to protect the X-Bank application, management tools, and operations against disaster? Do those plans provide for recovery within an acceptable period and to a sufficiently complete degree? Are those plans tested?
BS12-Compliance	Is X-Bank aware of and in all respects in compliance with relevant legal requirements? Does X-Bank have a compliance officer and does that officer have sufficient access to sources of legal expertise? Is all X-Bank software properly licensed? Is the project in compliance with all relevant X-Bank policies?
X-Bank1-Application	Is user data properly protected within the X-Bank application? Are system limits strictly controlled? Is access to the X-Bank application by both users and administrators suitably controlled? If unauthorized access does occur is the intruder's ability to do damage limited? Has the chance of system failure been minimized by proper capacity planning, an established acceptance procedure for new releases, and good housekeeping practices, including reliable backup procedures?
X-Bank2-Database	Are access rights to the database appropriate to each data function? Is particularly sensitive data securely encrypted? Is the database protected against corruption and destruction? Is the database sufficiently protected against tampering and is evidence of tampering preserved, if such occurs? Does backup of the database contents introduce any additional risks and are they properly controlled? Is the database recoverable? Has recovery been tested?
X-Bank3-Logging	Are logs created where appropriate in the system? Are those logs complete, incorruptible, and securely stored? Are they readable? Are they sufficient to guarantee non-repudiation of user and administrator activities? Where appropriate, is a process in place to analyze logging data? Does that data introduce any additional risks and are those risks properly controlled?
X-Bank4-Network Management	Is the application hosted in a secure environment and by a reputable hosting company? Are external connections from the host to external service providers and to X-Bank itself secure? Is the division of responsibility and chain of command for managing the network clear?
X-Bank5-Outsourcing	Are the additional risks posed by temporary and permanent outsourcing recognized? Are those risks addressed in the relevant SLAs and contracts? Can contractor compliance with agreed-upon security measures be accurately monitored? Have suppliers conducted their own sufficiently thorough risk assessments?

For each category an overall statement of risk is offered and controls are then discussed, first in general, then point by point. Each control is assigned to one of three classes:

1. Existing: This control has been put in place and tested. Each existing control is assigned to a specific functional role: whomever fills that function is responsible for maintenance of that control indefinitely.
2. Under Development: This control is currently being developed. Each such control is assigned to a specific person: regardless of role or title, that person is responsible for overseeing development of that control. (These controls appear in green.)
3. Possible Future Development: This control is being considered for future development; no responsibility is assigned. (These controls appear in blue.)
4. No Control Planned: Those risks for which no acceptable control is either available or immediately planned must be accepted; unless otherwise noted *responsibility for that decision is assigned to T Friedman, Project Manager*. In addition, an explanation of why a risk is judged acceptable is provided for all accepted risks: see Appendix 1: Statement of Acceptance of Risks. **Periodic re-review of all accepted risks is the responsibility of the X-Bank Chief Technical Officer, as is maintenance of this document.** (All such risks appear below in red.)

1.1: Executive Summary

This section summarizes overall risk status, highlighting areas of particular concern.

2: System Overview

This section briefly introduces the X-Bank system and related technologies. For a more complete discussion of functionality consult the relevant documents listed in Appendix 2: Bibliography.

3: Business Continuity Management

Statement of Risk: Continuity of the X-Bank system can be interrupted either by preventing the application from being served via the Internet or by cutting the connection between the application and the tools used to control it. In the former case, downtime means missed opportunities to sign up new users and can result in a loss of trust among existing users. If of extended duration, downtime of the application can lead to wider public notice and negative publicity, and can also produce interruptions in processing cycles within the application; such an extended loss of service will almost certainly diminish user trust in the system. If the connection between the application and IT Operations is broken the system will operate autonomously but control of the system will become impossible. If disaster strikes the X-Bank offices directly, then both control of the system and the ability to perform such tasks as fraud analysis will be effectively suspended. The system can always be shut off altogether by ordering the hosting

Dr. AT Shuldiner, Basel Consulting
alec@baselconsulting.com

company to shut down the production servers, but in the event of a severe disaster communications between X-Bank and the host could be thrown into disarray thus allowing the system to run untended for some time. If a bug or major fraud attempt should take place during this time X-Bank would be unable to respond to limit the damage.

General Controls: If disaster strikes our baseline response will be to recover the production environment from external backups. If the production environment is totally compromised we will serve the application from the test environment. If both are inaccessible we will use existing build instructions to install the application on freshly sourced hardware.

Status	Controls	Responsibility	Comments
Controlled	1. Essential system data is backed up in two physically and logically separate locations. 2. Backup uploads of all necessary elements of the application are stored apart from the Test and Production systems. 3. Complete documentation necessary to rebuild and restore the system is stored with the backup uploads.	IT Operations Manager	Backup and offsite storage of X-Bank operational information is addressed in the Risk Assessment, Operational
Under development	1. Marketing's disaster response plan only partially specified.	1. M. Menage	M. Menage has requested that Corporate PR oversee this function
Possible future development	1. Develop and implement detailed, case-based continuity plans. 2. Purchase insurance or otherwise hedge risk.	N/A	N/A

Accepted Risks: Failure of connection to Online Consumer Information Services will delay user validation. Failure of connection to Payment Processor NV will force operations to use the Electronic Banking system and could eliminate credit card functionality; if the EB system fails simultaneously certain transactions could become impossible to process. Failure of the Main Administrative Tool (either the software or the connection) could make Operations miss a transaction processing window; longer-term failure could make it impossible to conduct Customer Service or Fraud Prevention properly and could affect administration of the system. No provisions for insurance have been made.

4: Appendices

4.1: Appendix 1: Statement of Acceptance of Risks

Acceptance of risks directly associated with the production environment itself is assigned to the X-Bank Chief Technology Officer. Acceptance of all other risks is the responsibility of the Project Leader. The following table shows this division of responsibility and the explanations of acceptability for each stated risk.

Area of Risk	Risk	Responsibility	Explanation of Acceptability
BS11-Business Continuity Management	1. Failure of Online Consumer Information Services connection will delay user validation. 2. Failure of Payment Processor NV connection will force operations to use the Electronic Banking system and could eliminate credit card functionality; if the EB system fails simultaneously certain transactions could become impossible to process. 3. Failure of the Main Administrative Tool (either the software or the connection) could make Operations miss a transaction processing window; longer-term failure could make it impossible to conduct Customer Service or Fraud Prevention properly and could affect administration of the system. 4. No provisions for insurance have been made.	T. Friedman	These partial failures in external connections access (1, 2) limit the ability of X-Bank to deliver its services to its users but do not make it impossible to do so altogether: any such failure can be communicated to users (via robust email channels) as appropriate to limit negative perceptions. Under anything but extreme circumstances such failures should be rectifiable within a matter of hours or days at most, and such downtime is considered acceptable for the purposes of this initial commercial launch. Failure of the MAT (3) is believed to be very unlikely, and replacement of both the MAT software and hardware is easily and quickly done in the event of failure. If the project attains a longer time horizon insurance will be considered (4).

Dr. AT Shuldiner, Basel Consulting
alec@baselconsulting.com

These risks are explicitly accepted by X-Bank management as indicated by the signatures below:

Written Name, Title	Signature	Date

Written Name, Title	Signature	Date

[EOF]

Dr. AT Shuldiner, Basel Consulting
alec@baselconsulting.com