Internet Banking

Burcin Darendeli
Mengjia Gu
Internet banking is also called Online banking or E-banking.

It allows customers of a financial institution to conduct financial transactions on a **secure** website operated by the institution, which can be a retail or virtual bank, credit union or building society.
The term Internet banking refers to the use of the Internet as a remote delivery channel for banking services. Services include the traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic online payments (allowing customers to receive and pay bills on a bank’s web site).
Pop Quiz

Bank Activities  Risk Level

- Communicative  Low
- Informational  Mild
- Transactional  High
Internet Banking Activities

- **Informational**
  - The basic Level;
  - Market information about the bank’s products and services;
  - Low risk.

- **Communicative**
  - Some interaction between the bank’s systems and the customers;
  - Controls should be in place to prevent any unauthorized attempt to access the bank’s internal network;
  - Mild risk.

- **Transactional**
  - Directly execute transactions with financial implications;
  - Bill payments and fund transfer;
  - High risk.
Where is it used?

- Home/office computer
- Personal laptop
- Cell phone
- Ipad
Who are the users?

- Customers who have registered with the institution for the service.
- Customers who want to do transactions by themselves instead of going to the banks/institutions in person.
- Customers who want an efficient service
Internet Banking Features

- View account balances
- View recent transactions
- Download bank statements
- View images of paid checks
- Transfer funds
- Pay to the third parties, including bill payments and telegraphic/wire transfers
- Loan transactions
The advantages of Internet banking

- Efficient
- Convenient
- Easy to manage
- Any time & anywhere
The Drawbacks of Internet Banking

- Take some time to set up and get used to an online account
- Some banks only offer online banking in a limited area.
- Limited service (i.e. traveler’s checks and cashier’s checks are not offered)
- May have security problems because of unstable systems
Big Picture of Internet Banking
Dataflow diagram for bank account customer

Client
Connect to Internet

Open Browser

Enter URL

Login

Account Info

SERVER

Forget Password

Password Retrieval page

JSP

DATABASE

View Transaction
Balance Transfer
Update Address
Pay Bills

Confirmation/error page for ①-⑤

Select from Menu
Architecture of Online Banking

Customer

Request (a form of JSP file)

Response (with data requested/Error message)

Administrator

Request (a form of JSP file)

Response (with data requested/Error message)

Application Server

(JDBC-ODB) Bridge Driver

Request/Reply for Customer/Administrator

Database
Internet Banking Modules

- Bank Account
- Credit Card Customer

DATABASE

- Bank Account Administrator
- Credit Card Account Administrator
The information criteria most relevant to an Internet Banking audit

<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectiveness</td>
<td>Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Concerns the provision of information through the optimal (most productive and economical) use of resources</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Concerns the protection of sensitive information from unauthorized disclosure</td>
</tr>
<tr>
<td>Integrity</td>
<td>Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations</td>
</tr>
<tr>
<td>Availability</td>
<td>Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria</td>
</tr>
<tr>
<td>Reliability of information</td>
<td>Relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities</td>
</tr>
</tbody>
</table>
## Internet Banking Security

<table>
<thead>
<tr>
<th>Security Criteria</th>
<th>Online-Banking Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks</td>
<td>Unauthorized access</td>
</tr>
<tr>
<td>Backup</td>
<td>Information disclosure/loss</td>
</tr>
<tr>
<td>Secure Platform</td>
<td>Lack of fame and credit</td>
</tr>
<tr>
<td>Safe Environment</td>
<td>Loss of Financial resources</td>
</tr>
<tr>
<td>Secure Client</td>
<td>Customers Complaint</td>
</tr>
</tbody>
</table>
Internet Banking Threats

- **Application threats**
  “in which the person committing the fraud appears to be a legitimate user of the online banking application, but is instead conducting illegal activities”

- **Network-based threats**
  “such as hacks, site-defacement attacks, denial-of-service attacks, and viruses and worms, which attack the core network and infrastructure”
Internet Banking Risks

- **Strategic Risk:**
  “Many senior managers do not fully understand the strategic and technical aspects of Internet banking.”

- **Transaction Risk:**
  “Most Internet banking platforms are based on new platforms which use complex interfaces to link with legacy systems, thereby increasing risk of transaction errors. There is also a need to ensure data integrity and nonrepudiation of transactions.”

- **Compliance Risk:**
  “This is the risk to earnings or capital arising from violations of, or nonconformance with, laws, regulations and ethical standards.”
Reputation Risk:
“A bank's reputation can be damaged by Internet banking services that are poorly executed (e.g., limited availability, buggy software, poor response).”

Information Security Risk:
“This is the risk to earnings and capital arising out of lax information security processes, thus exposing the institution to malicious hacker or insider attacks, viruses, denial-of-service attacks, data theft, data destruction and fraud. “

Credit Risk:
“This is the risk to earnings or capital from a customer's failure to meet his financial obligations.”
Internet Banking Risks

- Interest rate risk
- Liquidity risk
- Price risk
- Foreign exchange risk
- Third party security risk
“The board and senior management should establish effective management control over the risks associated with internet banking activities, including specific accountability, policies and controls to manage these risks.”
Security Controls

- Authentication
- Nonrepudiation
- Segregation of duties
- Network and Data Access Controls
- Transaction Verification
- Virus Protection
- Detection of Possible Intrusions
Legal and Reputational Risk Management

- Privacy
  - Privacy Policy

- Availability
  - Business Continuity and Contingency Plan

- Incident response
  - Incident Response Plan
Other Controls

- Controls in “Outsourcing”
- Controls in “Advertisements and website links”
- Customer Education
Common Myths and Misconceptions of Internet Banking

- Myth #1: “We have a firewall.”
- Myth #2: “Secure Internet banking is not our responsibility, we outsource it.”
- Myth #3: "Only authorized people have access to our network."
- Myth #4: “We have a disaster recovery plan and we do backups nightly.”
- Myth #5: “We had a security review and everything was fine.”
Objectives of Internet Banking Audit

- To gain an understanding of the bank's Internet Banking product line, transaction flow, and settlement processes.
- To ensure that adequate internal controls are in place to minimize errors, discourage fraud, and provide an adequate audit trail.
- To determine whether the board of directors has adopted effective policies for Internet banking and these policies and procedures are being followed.
- To determine if contingency and disaster plans are adequate.
- To determine if the bank complies with applicable regulations.
- To determine whether management has instituted controls that are appropriate to the type and level of risks arising from Internet banking.
What to Look

ISACA's Standards: Aspects to Review

- Organizational Aspects
- Policy Aspects
- Planning Aspects
- Information Systems Infrastructure Aspects
- Telecommunication Infrastructure Aspects
- Authentication Aspects
- Third-party Service Provider Aspects
**What to Look**

- A Sample Form
  [http://www.auditnet.org/docs/InternetBankingAP.pdf](http://www.auditnet.org/docs/InternetBankingAP.pdf)

---

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

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

- http://www.bits.org/publications/fraud/FraudInternetBanking.pdf
- http://www.auditnet.org/docs/InternetBankingAP.pdf
Questions