

B&Online Web site Requirements Specification

Version 2.0

Draft

December 2000

Ivan Networkski
IS Director
Brown & Donaldson

Table of Contents

TABLE OF CONTENTS	2
INTRODUCTION	4
1 PURPOSE.....	4
2 SPONSOR, CUSTOMERS (USERS) AND OTHER STAKEHOLDERS	4
3 SCOPE.....	4
4 CONSTRAINTS.....	4
5 DEFINITIONS, ACRONYMS AND ABBREVIATIONS.....	4
<i>Business Terms</i>	4
<i>Technical Terms</i>	5
<i>Program and Database Naming Conventions</i>	5
6 ASSUMPTIONS	5
<i>Need to be investigated</i>	5
<i>Unable to confirm</i>	5
<i>Fact</i>	5
FUNCTIONAL REQUIREMENTS.....	6
1 USER CHARACTERISTICS	6
<i>Actors</i>	6
2 FUNCTIONAL REQUIREMENTS	7
<i>Web Pages</i>	7
<i>Reports</i>	8
<i>External Interfaces</i>	8
3 DATA REQUIREMENTS.....	8
<i>Business Objects</i>	8
<i>High Level Business Object Model</i>	8
<i>Class Hierarchy</i>	8
<i>Legacy Data</i>	8
NON-FUNCTIONAL REQUIREMENTS.....	9
1 CODING STANDARDS	9
<i>Coding Style</i>	9
<i>Permitted Technologies</i>	9
<i>Restricted Technologies</i>	9
2 GRAPHICAL USER INTERFACE (GUI) GUIDELINES	10
<i>Page Size</i>	10
<i>Page Layout</i>	10
<i>Graphics</i>	10
<i>Text</i>	11
3 CONTENT.....	11
4 NAVIGATION	11
5 USABILITY AND ACCESSIBILITY	11
6 CULTURAL AND POLITICAL	12
7 PERFORMANCE	12
8 CAPACITY, SCALABILITY AND MAINTAINABILITY.....	12
9 RELIABILITY AND AVAILABILITY	12
10 COMPATIBILITY, PORTABILITY AND OPERATIONAL ENVIRONMENT(S)	13
<i>Production and Acceptance test environments</i>	13
<i>Demonstration and System test environments</i>	13
<i>Development and Unit test environments</i>	13
<i>Client-side environments</i>	13
11 BACK-UPS AND DISASTER RECOVERY.....	14

B&D Online Web site Requirements Specification

12 FILE AND DATABASE INTEGRITY	14
13 AUDIT.....	15
<i>Web Site Access</i>	15
<i>Web Application</i>	15
<i>Database (SQL Server)</i>	15
<i>3rd Party Endorsement</i>	15
14 SITE SECURITY	15
<i>Firewalls</i>	15
<i>DMZ Server Operating System (Windows 2000)</i>	16
<i>Intranet (Non DMZ) Server Operating System (Windows 2000)</i>	17
<i>DMZ Services e.g. Web Server (IIS)</i>	17
15 APPLICATION SECURITY	17
<i>Client</i>	17
<i>Internet Transmission</i>	18
<i>Web Application</i>	18
<i>Database (SQL Server)</i>	18
16 LEGAL	19
17 MARKETING	19
FUTURE ENHANCEMENTS.....	21

Introduction

1 Purpose

In order to be competitive in the US Brokerage market, B&D feels that it needs to be able to offer it's existing and future clients the opportunity to trade US equities online. This project's goal is provide a basic online trading Web site (which can be enhanced in the future) ASAP.

Note, This document is based of the IEEE 830 standard for Software requirements and describes the desired product, but does not attempt to specify the details of when, who or how much the product will be built, this information is covered in the corresponding project planning documentation.

2 Sponsor, Customers (Users) and other Stakeholders

Donald Thump (CEO of B&D) is the Sponsor of the Project. Other Stakeholders of note include, Julie Sold (VP of Sales), Jack Bond (COO's Representative) and Ivan Networkski (IS Director).

The anticipated Customers of the product (B&D Online) are initially expected to be B&D's existing Customers. Specifically Mutual fund managers and wealthy private clients with varying degrees market trading experience.

3 Scope

See the associated "B&D Online Business Processes" document, which outlines the processes (computer and manual) that will need to be put in place for the B&D Online Web site to be implemented. Also, the associated "B&D Online Context Diagram" (in PowerPoint 97/2000) provides a high level overview of how all of the processes are dependent upon each other

4 Constraints

- Total costs for the development and running of the Web site for the first year must not exceed \$10 million
- A prototype of the Web site must be demonstrable within 1 month of project initiation
- The Web site must be operational within 2 months of project initiation
- The Web site will be free to existing clients
- Clients will not be willing to install personal certificates, personal firewalls nor be willing to authenticate themselves using some sort of biometric device or smartcard
- The project will have to be resourced with B&D's existing staff

5 Definitions, Acronyms and Abbreviations

Business Terms

See B&D's corporate glossary for a list the terms used in the brokerage business that are not normally found in "everyday" language, but will be referenced within this document e.g. Security - An investment instrument issued by a corporation, government, or other organization that offers evidence of debt or equity

B&D Online Web site Requirements Specification

Technical Terms

See B&D's IT glossary for a list of technical terms/acronyms used in the B&D Online product that are not normally found in "everyday" language, but will be referenced within this document e.g. ASP - The term "ASP" has 2 distinct meanings - Microsoft has a technology (Active Server Pages) that allows developers to develop dynamic Web sites quickly. An industry term to describe companies (Application Service Providers) that offer individuals or enterprises access over the Internet to application programs and related services that would otherwise have to be located in their own personal or enterprise computers

Program and Database Naming Conventions

B&D's standard naming conventions (see B&D naming conventions document) will be used for this project.

6 Assumptions

Need to be investigated

Assumptions that can be investigated and found to be true or false, the assumption then becomes a known requirement/constraint or is removed

- The vast majority of B&D's existing clients will view the Internet using:
 - A high speed (ISDN or better) Internet connection
 - With at least a:
 - 15" monitor
 - 800x600 screen resolution
 - 256 colors
- Are B&D's clients willing to pay for access to premium services? And if so how much?
- Are Advertisers will be willing to pay to advertise on the B&D Web site? And if so how much?

Unable to confirm

Assumptions that can not be investigated until after the project is complete (if ever)

- More people will use the B&D Online Web site, if the Web site does not require the viewer to enable cookies
- During the first year of operation, the B&D Online Web site will not need to be ported to another ISP and/or system software platform e.g. Unix or 2 tier Windows NT
- Initial peak load is expected to be 10 concurrent users, with each user requesting a new page every minute
- Clients will be unwilling to install client-side certificates and would object to B&D probing their machines to read "private" information e.g. MAC address (Ethernet card), CPU serial # (Pentium III chips), O/S serial #'s or Network node names

Fact

- As of this month 90+% of B&D's "Brochureware" Web site visitors use Microsoft 4.x (or higher) or Netscape 4.x (or higher), only 2.5% are AOL users
- A significant percentage (10%) of B&D's exiting clients spent a significant portion of their time outside of the U.S.

Functional Requirements

1 User Characteristics

The associated series of Use Case descriptions (Word 97/2000) and Use Case diagrams (PowerPoint 97/2000) specify, the interactions between the Actors (Customers, Internal Admin and/or other Computer systems) and the parts of the previously documented "B&D Online Business Processes" that will be directly supported/implemented by the B&D Online Web Site.

Actors

The list of Actors would potentially include:

- Novice/First time investors
- Novice computer/Internet users
- "Techie" users
- "Day traders"
- "Savvy"/Experienced Investors
- Passive investors - no trading
- Financial newspaper readers
- Foreign/International investors
- Competitors clients
- Potential new B&D clients
- Existing B&D clients
- Investors with poor vision
- External mutual fund managers
- B&D analysts
- B&D brokers
- B&D employees
- B&D senior management
- B&D securities auditors
- B&D webmaster
- Other B&D computer systems (legacy systems) Other companies Webmasters
- Business partners (including ISP's) and supply chain vendors
- Business partner employees
- CEO's and CFO's of companies that are traded
- Analysts at other research firms
- Stockbrokers at other brokerages
- Tax accountants
- Trade press/Media (Reuters, PRNewsWire, BusinessWire etc.)
- Web site raters/critics
- Small business owners, CFO's, 401k, ESOP administrators/trustees
- (Legal) Regulators (e.g. SEC, IRS) and B&D's Internal legal department
- External auditors (e.g. CPA's)
- Lawyers (e.g. class action)
- Hackers
- Competitors
- Children/Student - school/college research projects to bogus accounts
- Potential new hires
- B&D customer service/tech support
- B&D's Testing (Diagnostic) team
- Search engines
- "Agents" - computers from other companies

B&D Online Web site Requirements Specification

- Banks, Federal Reserve, Stock Market computer interfaces

Note: Many of these potential actors could be merged if their site usage turned out to be the same

2 Functional Requirements

Web Pages

The associated "High Level Site Map" specifies the Web sites core pages and the main navigational links between them.

For each Web page see the associated "Page floorplan" and supporting description (in PowerPoint 97/2000). The following is an example of the layout for a Page Specification:

Page ABC

- Short descriptive overview of Web page
- Page name/Bookmark: "Research & Quotes"
- Page Level Cascading Style Sheet (CSS) (if different to Web site CSS i.e. bd.css) e.g. page.css
- Meta Tags e.g. Brown & Donaldson, Online trading etc...
- Initial Focus Point (Tab starting point) e.g. Component #4 - User log-in
- Secure transmission required (Y/N)

Supporting documentation for any non-visual page component will also be included.

Note, each page component on the "floorplan" will be assigned a unique # (typically ordered top-left to bottom-right), the supporting description will then reference each page component by #:

Page Component #1 - XYZ

- Purpose (brief description of the component)
- Link (External, Internal, Anchor, Re-post)
- Mouse-roll text (a.k.a. roll-over)
- Component level CSS (optional) e.g. component.css
- Client-side processing e.g. drop-downs, edit checks
- Server-side processing e.g. Database processing needed to populate component or performed as a result of clicking on the component - specify default sort order if more than one record is to be returned

Any multi-page transactions must be able to handle (or degrade gracefully) any of the following user initiated events mid-way through the transaction:

- User clears disk and/or memory cache
- User uses the Go and/or History buttons to revisit previous pages out of synch
- User uses the Browser's Reload button
- User resizes the Browser window
- User aborts (never finishes) transaction
- User takes an extended coffee break e.g. 30 minutes
- User resets their PC's clock (backward or forward)
- User uses two Browsers (same brand and version) to perform the same transaction, "flip-flopping" from one Browser to the next
- User uses two or more Browsers (same brand, different versions) to perform the same transaction, "flip-flopping" from one Browser to the next

All Date/Times should be based on the Web sites clock (Web server or Database server) not on the clients

B&D Online Web site Requirements Specification

Reports

For each required Report, see the associated "Report floorplan" and supporting description (in PowerPoint 97/2000).

External Interfaces

For each interface to an external system, see the associated interface specification and supporting description (in Word 97/2000).

3 Data Requirements

Business Objects

The associated "D&B Online Business Objects" document (in Word 97/2000) itemizes the high level Business Objects (attributes and methods) that the B&D Online database will be expected to persistently store.

High Level Business Object Model

The associated "B&D Business Object Model" (in PowerPoint 97/2000) shows the relationships between instances of the high level Business Objects.

Class Hierarchy

The associated "B&D Class Hierarchy" diagram (in PowerPoint 97/2000) shows the relationships between the Object classes that are used to insatiate instances of the Business Objects.

Legacy Data

The new B&D Online Web site must be integrated into the existing back office legacy (Mainframe) stock trading applications.

Non-Functional Requirements

1 Coding Standards

Coding Style

- Visual Interdev 6.0 will be used to code all source code
- All Web pages should be W3C HTML 4.0 compliant
- All HTML code must should be Bobby Level 1 (cast.org) Accessibility compliant
- All Client-side scripting should be W3C JavaScript 1.2 compliant
- All Style Sheets should be W3C CSS Level I compliant, CSS Level 2 extensions are not to be used
- No proprietary (Microsoft or Netscape) HTML/JavaScript/CSS tags are to be used
- All server-side scripting should be coded in VBScript 5.0
- All Database calls should be coded with SQL via ODBC.
- All development/testing source code will be document/commented with standard module headers (thereby making maintenance/debugging easier), especially for server side includes e.g.:
 - Module name
 - Original author
 - Date initially written
 - Language and version
 - B&D Copyright
 - Enhancements/changes log - who/when/whyNote: For performance and security reasons, the production version (as seen by the user) will not contain this information (with the exception of the copyright, which should be placed in the "Copyright" meta tag).
- Where possible HTTP- EQUIV Meta tags are to be avoided (some browsers no not support this type of Meta tag)
- No absolute links are to be used for internal Web pages
- All client-side edit checks are to be redone on the server-side (since the user could turn off the client-side scripting language)
- Application error messages should be informative to the client, but no so descriptive as to useful to a hacker trying to figure out the internal workings of the application

Permitted Technologies

In addition the technologies implicitly permitted in the Coding Style section and other sections of this document, the following technologies are also permitted:

- Cookies (session and persistent - no expiration date)
- Server Side Includes (SSI and XSSI)
- Tables (nested tables may be used)
- Forms
- JavaScript Pop-ups

Note, the Web site should degrade gracefully if the client's browser does not support any of these technologies.

Restricted Technologies

- Client-side Java Applets/Servlets, Java Applications or ActiveX controls. This diminishes the benefits of "signing" the code, therefore developers will not be required to sign the code
- Server-side Java Beans (EJB), Java Servlets, Java Applications or ActiveX controls
- Framesets

B&D Online Web site Requirements Specification

- Java Style Sheets (JSS) are not to be used
- CGI scripts
- No Mailto's are to be used (all contact will be via Forms)
- XML vocabularies are not to be used (this may be reviewed in future release)
- WML will not be directly supported in the initial release
- No client-side Plug-ins (3rd party or B&D developed) will be required
- Multiple domains will not be used, the entire contents of the Web site will reside within a single domain

2 Graphical User Interface (GUI) Guidelines

Page Size

- All pages should ideally be viewable without the need for horizontal scroll bars when viewed with via a monitor with 800x600 pixel screen resolution. Assume an effective page size of 750x500 (50 and 100 pixels being reserved for the browser frame and vertical scroll bar). However, to make the Web page printer friendly the available width will be restricted to 660 (a future release of the Web site may have custom "Printer friendly" Web pages designed for US Letter length and A4 width - lowest common denominator approach)
- No single page should be longer than 2 page lengths i.e. 1000 pixels
- No single page download should exceed 100k

Page Layout

- The B&D corporate color palette will consist of 16 core "browser safe" colors (including white and black)
- No page should use more than 256 colors (including dithering colors)
- White should be used as the default background color
- Today's date will be displayed on each Web page (Tuesday, September 05, 2000 format)
- B&D Copyright will be displayed at the bottom of each Web page
- All page component sizes should be specified by a % of the page, rather than an absolute # of pixels
- All dropdowns controls should by default be sorted alphabetically and be wide enough to view all probable selections

Graphics

- .jpg's are to be used for photographic images and should be compressed to the smallest size possible while maintaining a clear picture, use of the progressive feature should be avoided (they are not supported by 2.x Browsers and are problematic in some 3.x versions) except for exceptionally large files.
- .gif's (currently do not use .png's) are to be used for non-photographic images
- Where possible all image files should be composed of 8x8 pixel blocks (gif's are downloaded in blocks of 8x8 pixels)
- All image files should use a DPI of 72
- No .gif's should use more than 16 colors (including differing colors) the main colors should be selected from the B&D corporate palette and "saved as" with as few colors as possible
- .gif's may be saved with Transparency but should not be interlaced
- Sponsor logo gifs must be 125x125 pixels in size (in advertising lingo this is refereed to as an industry standard "Square Button") and use no more than 16 colors
- All graphics must be assigned an <ALT> tag

B&D Online Web site Requirements Specification

- Maximum of 1 animated image per page (more than one .gif file is permitted if they are visually located next to each other, thereby appearing to the viewer to be a single animated area)
- Client-side image maps can be used to improve download times, but Server-side image maps are not to be used

Text

- All text will use the B&D corporate Cascading Style Sheet (W3C CSS level 1), named bd.css
- Assume only proportional fonts are to be used. No fixed-width fonts are to be used
- No Embedded fonts are to be used
- No tiny fonts are to be used i.e. point size < 8
- No obscure fonts are to be used e.g. Haettenschweiler
- All Dates, Telephones #, Addresses and Currency amounts should be displayed using standard U.S business formats e.g. mm/dd/ccyy or ccyy format, however input fields should be able to accept international variations e.g. alphanumeric postal codes

3 Content

- All text (Initial release) must be in U.S. English - No Spelling mistakes are permitted
- The narrative content of any edited article should be understandable by a viewer with a reading age between 16 and 25, lower than 16 and the "average" investor may find the article too simplistic, higher than 25 and a significant percentage of viewers may find the article too challenging
- Real time data (e.g. stock quotes) should typically not be more than 30 minutes old
- No content that is copyrighted or trade marked by another organization is to be used without explicit written agreement by that organization
- Non real time content will be updated daily (e.g. Market news articles)

4 Navigation

- All links will use browser default colors
- Each page must have a meaningful page name and be Bookmarkable
- The Site map must match the actual Site Navigational Hierarchy
- The bdonline.com Web site should be available using either <http://www.bd-trade.com> and/or <http://bd-trade.com>
- There should be no internal broken links
- The Web site should have a customized (user friendly) error page e.g. 404 page not found
- Internal URL links should reuse the existing Browser instance (the exception would be any help pop-up Windows)
- External URL links should spawn a new Browser
- All Web pages should be reachable within 5 clicks of the Home page (using a scroll bar counts as a click), excepts include pages that are part of a multi page transaction and should not be reached without traversing other pages within the transaction

5 Usability and Accessibility

- The Web site must "degrade gracefully" for users who have a browser that is does not provide the functionality needed by the Web site (e.g. Javascript) due to either the browser not having that functionality (e.g. an old version) or because the viewer decided not to enable that particular feature (e.g. cookies turned off)

B&D Online Web site Requirements Specification

- The Web site must explain B&D's policy of privacy (the legal department is currently working on this)
- The Web site's Browser requirements must be posted e.g. 4.x (or higher) generation of browser JavaScript, Session Cookies are required - persistent cookies, style sheets, 800x600 resolution (min), 256 colors (min) recommended for optimal performance
- The Web site should be Bobby Level 1 (www.cast.org/bobby/advanced.html) Accessibility compliant
- Mandatory data entry fields may be flagged with a visual cue e.g. highlight in red
- The Web site should be intuitive - Once the Web site goes live, if more than 10% of the emails received by B&D are from viewers having trouble using the Web site, the Web site will be deemed to be non-intuitive and would become a candidate for redesign

6 Cultural and Political

- While the Web site may require users to be able to read English, it should still be comprehensible to users who do not speak U. S English as their first language, therefore common U.S phrases or expressions should not be used if it is possible for the international user to misinterpret their meanings e.g. "Buy this stock" maybe misinterpreted as a recommendation from B&D rather than merely a convenient button for actually buying a stock online
- Public companies that compete with B&D will be available to be bought and sold online
- The B&D online Web site will not (current release) contain any stock purchase/sell recommendations
- The B&D Web site will not interrogate the clients machine to determine client settings e.g. screen resolution, Ethernet MAC address or Pentium III serial # etc.

7 Performance

- When accessing any not database Web page from anywhere in the continental 48 states, 95% of the pages requested (while the Web site is up) during U.S business hours (m-f 8-9 EST) using an average PC with a 28.8kb modem that is connected to a tier 1 ISP and a 5.x generation MS IE/Netscape Windows based Browser must completely load within 10 seconds
- The requirement for database orientated Web pages is 20 seconds

8 Capacity, Scalability and Maintainability

- The selected System Software/Application architecture should support B&D's expected audience for the next 6 months (assuming minor hardware and system software upgrades)
 - Initial - 3000 concurrent users generating 100 Web page requests per second
 - 6 months – 50% increase
 - 12 months – 100% increase
- The Database should be able to handle 100MB of data
- The Web logs should be able to handle 100MB of data
- Network bandwidth should be able to handle 1MB per second of data
- Mirror sites are not available
- Server clustering is not available (currently unaffordable)

9 Reliability and Availability

- Typically 24x7 availability (this includes access to accurate real time content i.e. during market hours stock quotes should not be more than 30 minutes old)
 - 97% update during core hours (4.00am to 10.00pm EST Mon-Fri)

B&D Online Web site Requirements Specification

- 90% update during non-core hours
- Mean time to repair (MTTR) 1 hour
- Maximum one 10 hour plus outage per month
- Server memory leakage's must not exceed 10k per day
- External broken links should be detected and fixed/removed within 24 business hours

10 Compatibility, Portability and Operational Environment(s)

Three server-side platforms will be support (production/acceptance test, demonstration/system test and development/unit test):

Production and Acceptance test environments

- The production Web site will be hosted by Bell South in Atlanta and viewable by anyone in the world using a Internet enabled Browser
- Multiple domain names (e.g. bdonline.com and bd-online.com) will "point" to a single IP address
- A second IP address (no domain name) will be available for acceptance testing
- The production and acceptance testing environment will reside on the same physical machine:
 - A single Intel based server running Windows NT 4 sp6, IIS 4 and SQL Server 7 (MS ODBC driver 3.70) or Access 2000 MDE (MS ODBC driver 4.00)
 - All files will reside on the same hard drive, the hard drive will be mirrored and hot swappable
- B&D's existing Windows based Configuration Management system will be used to control check-in and check-out procedures for source code and content management. Configuration Management procedures and file directory structures will be documented
- Old versions of software and content will be removed from the production server has soon as the new release has been successfully implemented
- All server Dates/Times should be synchronized with the U.S governments official Eastern Standard time (EST)
- Web server must accept requests formatted as either <http://www.xyz.com> and <http://xyz.com>
- All unused floppy drives, firewire ports, USB ports, parallel ports, external SCSI connectors and external IDE connectors will be removed/disabled from all production servers

Demonstration and System test environments

- The production and acceptance testing environment will reside on the same physical machine:
 - A single Intel based server running Windows 95/98, MS PWS and Access 2000/ODBC
 - All files will reside on the same hard drive

Development and Unit test environments

- The Development environment will use (as far as is feasibly possible) the same System Software as the production environment

Client-side environments

Web pages should be accurately rendered by all on the U.S. general release versions of the following Browser software:

- Netscape Navigator 4.0 and 4.x (where x is the last release)
- MS IE 4.0 and 5.x (where x is the last release)

B&D Online Web site Requirements Specification

Running any of the following U.S. general release client Operating Systems:

- Windows 95
- Windows 98 2nd Edition
- Windows Millennium
- Windows NT 4 Workstation (no support packs)
- Windows 2000 Professional

Note: Y2K upgrades may be installed

Assuming Hardware is sufficient to efficiently run any of these combinations e.g. Windows NT will not be installed on a 486 machine

11 Back-ups and Disaster Recovery

- The Web site should be able to operational within 1 hour of a systems crash and 1 day of a catastrophic event e.g. natural disaster like a hurricane or earthquake
- No confirmed transactions should be lost
- Arrangement with a second ISP should be made to host the Web site, in the event that the primary ISP's hosting location becomes unavailable (e.g. Hurricane)
Note, this site could be used as a System Test environment
- The ISP site must have a Uninterruptible Power Supply (UPS)
- At the end of each day, the Developer team will back-up the source code for the entire Web site into a single Zip file located on a B&D network drive. Periodically a copy of the zip file will be transferred to a off-site back-up location e.g. the project managers home's home
- An "Intruder response" policy will be developed to handle the scenario of a hacker gaining access to some portion of the Web site

12 File and Database Integrity

The following procedures will be used to ensure that the Web site's program files and data files/databases are not get corrupted:

- All static program files will reside under a Directory called "DBOnline". The contents of this directory will be burnt on to a CD-ROM thereby allowing these programs to potentially executed directly from a CD-ROM drive rather than from a traditional rewriteable Hard Drive (for performance reasons, the production environment may actually still use a traditional hard drive)

Sub-directories would include:

- Images
- Scripts
- Templates
- Database
- Pages

Note, for security purposes the names of these directories may be changed prior to the Web site going into production

- All dynamic/temporary files will reside under a Directory call "DBOnlineTemp". The contents of this directly will on a regularly basis be deleted and re-initialized
- The Database design will use a combination of Foreign keys, Rules and Triggers to enforce "Referential Integrity" (RI) on all relational database tables
- All aborted/incomplete transactions must be rolled back

B&D Online Web site Requirements Specification

13 Audit

Web Site Access

Standard B&D file promotion/configuration procedures (see associated B&D file promotion/configuration procedures document) will be enforced for all production B&D Web site servers. Special attention should be paid to logging attempts to access unauthorized resources and the precautions taken to ensure that the audit trails themselves are not altered/deleted.

Web Application

Audit trails in accordance with regulatory guidelines will be implemented. These application audit trails will be initially maintained within the database and subsequently migrated to an off-site medium, where they will be stored for a minimum of 7 years (unless regulations require otherwise).

Database (SQL Server)

By default each table within the database will have the following audit attributes attached to each record:

- Date/Time record created
- User Id of creator
- Date/Time record last updated
- User Id of updatator

3rd Party Endorsement

B&D will seek to have the B&D Online Web site endorsed by one or more of the following outside auditors:

- TrustE (truste.com/etrust.com)
- BBBOnline (bbbonline.com)
- WebTrust (cpawebtrust.com)

14 Site Security

The Bonline Web application will be installed on a collection of servers and network connections collectively known as the Web site. To ensure that the security mechanisms built into the Web application cannot be circumvented, it is extremely important to ensure that the Web site upon which the Web application is installed is itself secure. Therefore the standard security policy used by B&D for any server/network that is connected to the "outside World" will be implemented. The following is a summary of the "Web centric" portions of this policy:

Firewalls

The Web site will implement a standard 2-layer firewall. The first layer will be a network level (packet filtering) firewall designed to protect the Web server and any other servers that need direct access to the Internet. The second layer will be an application level (proxy server) firewall designed to provide extremely tight security even if performance is impacted. The area between the two-firewall layers is typically referred to as a Demilitarized zone or DMZ.

Basic access control requirements (rules) for the first layer include:

- Only TCP/IP traffic is permitted, non-IP and UDP/IP traffic should be dropped

B&D Online Web site Requirements Specification

- Any inbound IP packet that “claims” to have originated from a machine located within the Web site or intranet should be dropped
- Any outbound IP packet that “claims” to have originated from a machine not located within the Web site or intranet should be dropped
- Any inbound IP packet that is destined for any machine other than a machine within the DMZ should be dropped
- Only requests to/from port 80 (HTTP), 443 (HTTPS) or 21 (FTP) are to be permitted, all other requests are to be dropped
- Any vendor default user IDs, passwords or remote login capabilities have been disabled
- The default router “banner” has been replaced with a B&D legal notice

Basic access control requirements (rules) for the second layer include:

- Only TCP/IP traffic is permitted, no non-IP or UDP/IP traffic
- Only traffic that originated from a DMZ machine is permitted into the intranet
- Only traffic intended for a machine in the DMZ is permitted to exit from the intranet
- IP application and port combinations that are permitted include: HTTP (80), HTTPS (443), SMTP (25) and NetBios (135-139)
- Any vendor default user IDs, passwords or remote login capabilities have been disabled
- The default router “banner” has been replaced with a B&D legal notice

In addition, B&D’s ISP will be contacted to determine what capabilities the ISP has in place to minimize the effect of a “denial of service” attack on B&D’s Web sites and whether any of the ISP’s routers that are “up-stream” from the B&D Web site can be configured to act as an additional network layer firewall.

DMZ Server Operating System (Windows 2000)

- The most recent version of Windows 2000 will be installed, including any service packs and security patches
- Each machine will have its own local administrator account, no two accounts will use the same user ID or password (see B&D’s security policy for further explanation of what constitutes a “strong” user ID and password)
- After 3 unsuccessful login attempts, the account will be locked out for 30 minutes
- Bios and screen saver passwords will also be implemented
- Any vendor default user IDs, passwords or remote login capabilities have been disabled
- Standard intruder misdirection and detection procedures should be implemented e.g.:
 - Do not install the Windows O/S in its default directory, instead install the O/S in a nondescript directory such as “Bitmaps” and place a tripwire in the default directory
 - Create a file named “passwords.txt” in a sub-directory called passwords, the file should contain a series of bogus Windows 2000 users ID’s and passwords and have an associated “tripwire”
 - Once installed checksums should be made of static directories and files
 - Before placing the server into production, tamper-proof backups (e.g. CD-ROMs) of the servers hard-drive should be made and stored off site and locally
 - The default Windows 2000 banners should be replaced with banners indicating that the machine is using another brand of O/S e.g. Linux, Sun UNIX etc.
- All directory and file privileges should be kept to a minimum
- Audit trails should be set to append only
- Each machine will be installed with 2 network cards (NICs), one card will be used to connect to the “outside World” via the network layer firewall and the other connected to the intranet via the application layer firewall
- Any unnecessary ports will be disabled on both NICs (Note, a valid application/port for one NIC may not be appropriate for the NIC)

B&D Online Web site Requirements Specification

- The machines internal IP address resolution tables should not contain entries for any machine located on the intranet. The entries for the firewalls and other DMZ machines should be static and not modifiable remotely
- DMS transfers should be prohibited
- All files hosted on each server will be scanned for viruses before they are made available to the public
- An Intruder Detection System (IDS) should be installed; since it is fairly safe to assume that these servers will be attacked regularly, rather than setting off a warning several times a day, the IDS's automated notification will be set to a low sensitive setting

A "Honey Pot" server will be set up in the DMZ, this server will have limited hardware resources and will not be connected to the intranet (even through the proxy server). However, some of the security settings on this machine will be lax and it's banner and directory structures will make it appear to be a server used by the testing department. In reality, the entire machine will be configured to act as one huge tripwire.

Intranet (Non DMZ) Server Operating System (Windows 2000)

A subset of the precautions used for the DMZ servers will implement. Two notable exceptions to this "rule of thumb" are:

- The IDS sensitivity setting will be set to high for all servers behind the second firewall or form part of the second firewall (proxy servers)
- Particular attention will be paid to ensuring that the passwords selected for administrative accounts on the DNS servers are exceptionally strong. Compromising these passwords could be the entire network domain at risk

DMZ Services e.g. Web Server (IIS)

- All public Web servers will be placed between in the demilitarized zone
- The most recent version of IIS will be installed, including any service packs and security patches.
 - A 128bit Key Web site certificate will be installed on each server to enable 128bit level https communication between the Web site and B&D's clients
 - The Web servers automatic directory services should be disabled
 - The default IIS banner should be replaced with banners indicating that the machine is using another brand of Web server e.g. Apache, Netscape, Weblogic etc.
 - CGI scripting will be disabled and all CGI scripts removed
 - SSI Exec command will be disabled
 - Reverse DNS lookups will not be implemented due to performance considerations
 - The system error message option will be set to provide minimal error messages, thereby helping to minimize the amount of information that a hacker could potentially learn about the internal workings of the Web site

15 Application Security

The overall security of the Web site will not be enforced using a single layer of protection, rather security measures will be adopted at all potential security breach points i.e.:

Client

The following procedures/techniques will be used to establish the "True" identity of the user attempting to access the B&D Online Web site via a Browser

- Clients must log on with a valid user ID and password before accessing the body of the Web site, the client will only be required to remember one user ID/password combination. The user

B&D Online Web site Requirements Specification

- Information used to authenticate a client (e.g. mother's median name, social security # etc) who has forgotten his/her user ID/password will be stored in a separate database to the database containing the client's accounts.

16 Legal

Since B&D is incorporated in New York state and the Web site will primarily be hosted on servers residing in New York city, all New York City, State and U.S Federal Laws & Regulations must be complied with. In addition, because clients around the world may view the Web site, the Web site must comply with the Laws and Regulations on the municipality, states and countries that B&D may legally conduct a meaningful amount of business e.g.

- U.S and International copyright laws must be complied with
- Other organizations trademarks are only to be used with their written consent
- Tax/Regulatory commissions will be collected where appropriate

17 Marketing

- Keyword and Description Meta tags (currently being defined by the Marketing department) should be used on all Public Web pages i.e. those Web pages that can be accessed without a valid login/password. All non-public Web pages should use:
<meta name="robots" content="noindex,nofollow">
- Within 2 months of the Web site going into production, the Web site should appear on the first results page of 8 out of 10 of the following Search Engines/Directories:

- Altavista
- AOL Netfind
- Excite
- HotBot
- InfoSeek
- Lycos
- Northern Light
- WebCrawler
- Yahoo
- Yellow Pages

For 8 out of 10 of the following keyword searches:

- Brown +Donaldson
- Online +Trade
- Online +Trading
- Online +Broker
- Brokerage
- Stocks
- Buy +Stocks
- Stock +Quotes
- NASDAQ
- NYSE
- Within 6 months of the Web site going into production, the Web site should have at least 10,000 unique visitors per day with 50% of all registered clients visiting the Web site at least once per week
- The production Web site must be able to provide current and prior data on pages hits per hour/day/week/month
- The production Web site must be able to count "click-throughs" to sponsor Web sites (reporting should be via the web sites Web log analysis tool)
- The additional domain names should "point" to the xyz.com Web site:
 - xyz.com

B&D Online Web site Requirements Specification

- xyz.org
- xyz.net
- xyz.co.uk (B&D currently has a subsidiary in London)
- xyz.org.uk

Future Enhancements

Possible enhancements that could be made to the Web site, but are currently consider out of scope e.g.

- Relevance and/or "fuzzy logic" search engine
- Support for multiple languages
- Support for video and or audio clips
- Wireless connectivity
- Chat events
- Low res/high res graphics option
- Utilize XML for data transmissions
- Replace CSS with XSL/ESL
- Expand audit trail and audit reporting
- "Email to a friend" feature
- "Printer friendly" feature