



Bernice Karn

Electronic Aspects of Business Transactions

IT, Software and License
Audits and Due Diligence

April 20, 2009

Agenda



- Meaning and purposes of IT due diligence
- Examples of typical business situations in which IT due diligence is important
- Specifics of IT due diligence in an M&A situation

Meaning of IT Due Diligence



- What is IT Due Diligence?
 - A subset of IP due diligence
 - An assessment of a company's key information technology assets

Meaning of IT Due Diligence



- What is IT Due Diligence?

- Determination of:

- What information technology assets exist
- What rights does the organizations have in relation to the assets
- Validity of the rights
- What encumbrances/prior rights exist against the assets
- What threats may exist in relation to the assets

Purposes of IT Due Diligence



- 3 Main Reasons for IT Due Diligence
 - Valuation
 - Risk management
 - Compliance

Specific IT Due Diligence Situations



- **M&A Transactions**

- Different considerations apply, depending on the deal context
 - Buying a company for its customer list is different from buying a company for its patent portfolio
- Acquiring an IT company
 - Does the company own what it says it does?
 - Are the systems properly licensed and reporting accurately?


Specific IT Due Diligence Situations



- M&A Transactions


- Acquiring any company that depends on IT systems
 - Are the systems properly licensed and reporting accurately?
 - Are the licenses assignable?

Specific IT Due Diligence Situations




- MI-52-109 – Certification of Disclosure in Issuers' Annual and Interim Filings
 - Non-venture issuers must implement and maintain disclosure controls and procedures as well as internal control over financial reporting to provide reasonable assurances as to reliability of financial reporting

Specific IT Due Diligence Situations



- **MI-52-109 – Certification of Disclosure in Issuers' Annual and Interim Filings**
 - Non-venture issuers must also provide reasonable assurance that information and reports will be recorded, processed, summarized and reported within required time periods and communicated to management to allow timely decisions regarding required disclosure

Specific IT Due Diligence Situations



- MI-52-109 – Certification of Disclosure in Issuers' Annual and Interim Filings
 - Control framework (e.g., COBIT) used by issuer to be disclosed


Specific IT Due Diligence Situations



- **Sarbanes-Oxley Section 302 Internal Control Certifications**


- Mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are “responsible for establishing and maintaining internal controls” and “have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared”

Specific IT Due Diligence Situations



- **Sarbanes-Oxley Section 404**
Assessment of internal control
 - Requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting (ICFR). This is the most costly aspect of the legislation for companies to implement, as documenting and testing important financial manual and automated controls requires enormous effort.

Specific IT Due Diligence Situations



- **Sarbanes-Oxley Section 404**
Assessment of internal control
 - The report must also “contain an assessment, as of the end of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting”
 - Internal control framework generally adopted to provide second certification

Specific IT Due Diligence Situations




- Payment Card Industry Data Security Standard
 - Set of comprehensive requirements for enhancing payment account data security to help facilitate the broad adoption of consistent data security measures on a global basis

Specific IT Due Diligence Situations



- Payment Card Industry Data Security Standard
 - Developed by the founding payment brands of American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International


Specific IT Due Diligence Situations



- Payment Card Industry Data Security Standard


- PCI DSS is enhanced as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption

Specific IT Due Diligence Situations




- Core PCI DSS principles are organized around:
 - Build and Maintain a Secure Network
 - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
 - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

Specific IT Due Diligence Situations




- Core PCI DSS principles are organized around:
 - Protect Cardholder Data
 - *Requirement 3:* Protect stored cardholder data
 - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks

Specific IT Due Diligence Situations




- Core PCI DSS principles are organized around:
 - Maintain a Vulnerability Management Program
 - *Requirement 5:* Use and regularly update anti-virus software
 - *Requirement 6:* Develop and maintain secure systems and applications

Specific IT Due Diligence Situations




- Core PCI DSS principles are organized around:
 - Implement Strong Access Control Measures
 - *Requirement 7:* Restrict access to cardholder data by business need-to-know
 - *Requirement 8:* Assign a unique ID to each person with computer access
 - *Requirement 9:* Restrict physical access to cardholder data

Specific IT Due Diligence Situations



- Core PCI DSS principles are organized around:
 - Regularly Monitor and Test Networks
 - *Requirement 10*: Track and monitor all access to network resources and cardholder data
 - *Requirement 11*: Regularly test security systems and processes

Specific IT Due Diligence Situations



- Core PCI DSS principles are organized around:
 - Maintain an Information Security Policy
 - *Requirement 12*: Maintain a policy that addresses information security

Specific IT Due Diligence Situations



- Privacy Compliance

- *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) governs the collection, use or disclosure of personal information collected in the course of commercial activity
- Provincial legislation in B.C., Alberta and Québec may also apply


Specific IT Due Diligence Situations



- **Privacy Compliance**

- Must ensure compliance with applicable privacy laws, both in-house and when information is transferred to a third party for processing
- The privacy statutes such as PIPEDA do not specify the specific IT measures that organizations must take in order to meet compliance standards

Specific IT Due Diligence Situations



- Privacy Compliance

- Principle 1 (Accountability), Clause 4.1.3 of Schedule I to PIPEDA:
 - An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Specific IT Due Diligence Situations



- Principle 7 of PIPEDA — Safeguards
 - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information

Specific IT Due Diligence Situations



- **Principle 7 of PIPEDA — Safeguards**

- Clause 4.7.1 - The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

Specific IT Due Diligence Situations



- **Principle 7 of PIPEDA — Safeguards**
 - Clause 4.7.2 - The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

Specific IT Due Diligence Situations



- **Principle 7, Clause 4.7.3 of PIPEDA**
 - The methods of protection should include
 - Physical measures, for example, locked filing cabinets and restricted access to offices;
 - Organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and
 - Technological measures, for example, the use of passwords and encryption.

Specific IT Due Diligence Situations



- IT Due diligence is relevant to privacy:
 - To ensure that Personal information is only used for the purposes for which it was collected
 - To manage disclosures of personal information
 - To ensure that information is protected by measures appropriate to its sensitivity level

Specific IT Due Diligence Situations



- IT Due diligence is relevant to privacy:
 - To detect data security breaches and prevent future breaches
 - To manage data retention programs
 - To discover conflicts in privacy policies in an M&A deal – may require privacy “work around”

Specific IT Due Diligence Situations



- **Outsourcing – OSFI Guideline B-10**
 - Sets out expectations for federally regulated entities (FRE) and their subsidiaries that outsource any of their business activities
 - FREs include Schedule I or II Bank; Trust and Loan Companies; Cooperative Credit Associations; Insurance Companies; Bank Holding Companies; Insurance Holding Companies; Cdn branch of foreign bank; Cdn branch of foreign insurance company

Specific IT Due Diligence Situations



- **OSFI Guideline B-10**
 - Provisions reflect prudent practices and although not statutory, FREs are strongly urged to follow them and use sound judgment in doing so

Specific IT Due Diligence Situations




- **OSFI Guideline B-10**

- Key provisions*:

- 7.1 – Due Diligence Process
- 7.2 – Policies and Procedures to Manage Risks Associated with Material Outsourcing
- 7.3.2 – Monitoring the Outsourcing Arrangement
- 7.3.3 – Monitoring the Service Provider

*http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b10_e.pdf

Specific IT Due Diligence Situations



- **OSFI Guideline B-10**
 - OSFI B-10 expects the FRE to audit the service provider's internal control environment in relation to outsourced services
 - OSFI B-10 recommends CICA 5970 (Auditor's Report on Controls at a Service Organization) or equivalent standard as appropriate

Specific IT Due Diligence Situations



- OSFI Guideline B-10

- CICA 5970

- Canadian standard published by the Canadian Institute of Chartered Accountants, denotes standard for measuring effectiveness of internal controls in relation to the preparations of financial statements

Specific IT Due Diligence Situations




- **CICA 5970 – Control Objectives**
 - Prevention and detection of error and fraud
 - Safeguarding of assets
 - Maintenance of reliable accounting records
 - Timely preparation of reliable financial information

Specific IT Due Diligence Situations



- Conformance with Cyber-Security Standards
 - Sensitive information is stored on computers that are connected to the internet

Specific IT Due Diligence Situations




- Conformance with Cyber-Security Standards
 - Leading standards:
 - ISO/IEC 27002 *Information technology - Security techniques - Code of practice for information security management*
 - Information Security Forum (ISF) Standard of Good Practice (SoGP)
 - The North America Electric Reliability Corporation (NERC) 1300
 - NIST 800-26

Specific IT Due Diligence Situations



- ISO/IEC 27002 - Best practices are grouped into the following categories:
 - Risk assessment
 - Security policy - management direction
 - Organization of information security - governance of information security
 - Asset management - inventory and classification of information assets

Specific IT Due Diligence Situations




- ISO/IEC 27002 - Best practices are grouped into the following categories:
 - Human resources security - security aspects for employees joining, moving and leaving an organization
 - Physical and environmental security – protection of the computer facilities

Specific IT Due Diligence Situations



- ISO/IEC 27002 - Best practices are grouped into the following categories:
 - Communications and operations management - management of technical security controls in systems and networks
 - Access control - restriction of access rights to networks, systems, applications, functions and data

Specific IT Due Diligence Situations



- ISO/IEC 27002 - Best practices are grouped into the following categories:
 - Information systems acquisition, development and maintenance - building security into applications
 - Business continuity management - protecting, maintaining and recovering business-critical processes and systems

Specific IT Due Diligence Situations



- ISO/IEC 27002 - Best practices are grouped into the following categories:
 - Compliance - ensuring conformance with information security policies, standards, laws and regulations
 - Information security incident management - anticipating and responding appropriately to information security breaches

Typical IT Transactional Due Diligence



- Transactional Due Diligence – Initial Considerations
 - What type of transaction is at stake?
 - Sale of a business vs. sale of an IT business?
 - What type of company is the target?
 - Longstanding stable enterprise or volatile organization with many transactions and high turnover?
 - What is important to the core business?
 - Software or hardware or are both important?

Typical IT Transactional Due Diligence



- Transactional Due Diligence – Initial Considerations

- Can we confirm the company's right to use IP?
 - Confirm right to use certain technologies, patents, copyrights and possibly trade-marks and/or domain names.
 - Is there any pending litigation?
 - Any third party rights triggered by the proposed transaction (e.g., options, rights of first refusal, event of default under security agreements)?

Typical IT Transactional Due Diligence



- Transactional Due Diligence – Initial Considerations

- IP valuation/Risk Management Issues?
 - Strength of rights in the marketplace
 - Whether rights extend to jurisdictions that represent important markets
 - Probability that unregistered rights will be successfully registered in future and will be enforceable
 - Licensed or sub-licensed to other parties/ defaults?

Typical IT Transactional Due Diligence



- Business vs. Legal Due Diligence

- IT professionals – their concerns:
 - Age and capacity of systems
 - Scalability, reliability, compatibility, maintainability
 - Knowledge transfer required?
 - Cost of acquisition/transfer

Typical IT Transactional Due Diligence



- Practical Issues to consider relating to IT
 - Key equipment
 - Vendor/target identity and status
 - Owned vs. leased vs. shared equipment/systems

Typical IT Transactional Due Diligence



- Practical Issues to consider relating to IT
 - Other ancillary equipment
 - Telecom systems
 - Mobile radio facilities
 - Fibre optics communication facilities
 - Microwave facilities, wireless fidelity networks,
 - Teleprotection/ telecontrol equipment
 - Test equipment
 - Administrative data handling facilities including real-time monitoring equipment, etc.

Typical IT Transactional Due Diligence



- Practical Issues to consider relating to IT
 - Software
 - Documentation - manuals, policies and procedures
 - User names and passwords
 - Copies of source code (or details of escrows) and decryption keys
 - System development plans

Typical IT Transactional Due Diligence



- Practical Issues to consider relating to IT
 - Software
 - System flow charts
 - Enterprise license issues
 - Transition services issues
 - Missing agreements

Typical IT Transactional Due Diligence



- Practical Issues to consider relating to IT
 - Exclusions
 - What is not being transferred or financed?

Typical IT Transactional Due Diligence



- Performance and Obsolescence Issues

- Copies of all written guarantees, warranties, assurances, etc. in any way concerning the workmanship and functionality of the equipment

Typical IT Transactional Due Diligence



- Performance and Obsolescence Issues

- Confirmation of the age, working condition and, where applicable, product version numbers/identifiers, of the equipment and a list and full details of any reported or perceived deficiencies or inadequacies or desired or appropriate upgrading of any such equipment

Typical IT Transactional Due Diligence



- Other Practical Issues
 - If a technology provider
 - List of inventories and ages
 - Accounts receivable and aging

Typical IT Transactional Due Diligence



- Other Practical Issues

- Other

- Real estate – hosting facilities – owned or leased?
- If leased – what documents comprise the tenancy – i.e., offers to lease, leases, amending agreements
- Permitted use of premises?
- Non-disturbance agreements from landlords
- Estoppel certificates

Typical IT Transactional Due Diligence



- Legal Due Diligence - What type of rights may be relevant?
 - Registrable Rights:
 - Patents for new inventions such as processes, machines, methods of manufacture, composition of matter, or any new and useful improvement of an existing invention

Source - <http://www.cipo.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/home>

Typical IT Transactional Due Diligence



- Registrable Rights:
 - Copyrights for artistic, dramatic, musical and literary works (including computer programs), and three other subject-matter known as performances, communication signals and sound recordings

Source - <http://www.cipo.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/home>

Typical IT Transactional Due Diligence



- Registrable Rights
 - Integrated Circuit Topographies for three-dimensional circuit designs
 - Trade-marks words, symbols, designs (or a combination of these), used to distinguish the wares and services of one person or organization from those of others in the marketplace

Source - <http://www.cipo.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/home>

Typical IT Transactional Due Diligence



- Registrable Rights

- Industrial designs visual features of shape, configuration, pattern or ornament (or any combination of these features), applied to a finished article of manufacture.
- Business names; domain names

Source - <http://www.cipo.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/home>

Typical IT Transactional Due Diligence



- **Non Registrable Rights**
 - Confidential information, know how
 - Contractual rights
 - Development agreements
 - Co-ownership agreements
 - Assignment of copyright
 - Licenses

Typical IT Transactional Due Diligence



- Confirm intellectual property rights held by business
 - Conduct ownership and status searches of all asset classes by relevant jurisdiction
 - Encumbrances
 - What liens, encumbrances, security agreements, or security interests which affect any of the equipment or software?

Typical IT Transactional Due Diligence



- Patents
 - Applicant, owner, inventor
 - NDAs, date of first disclosure
 - Non-competition agreements
 - Length of protection
 - PCT filings
 - Scope and validity of the claims
 - Related applications

Typical IT Transactional Due Diligence



- Patents
 - Status of examination process in each jurisdiction
 - Any security interests or assignments?
 - Potential/actual infringements by third parties
 - Potential/actual infringement claims from third parties

Typical IT Transactional Due Diligence



- Copyrights

- How to determine whether the target owns them?
 - Search registers by jurisdiction
 - Software
 - Obtain list of all individuals (both employees and contractors) who worked on the product and when
 - Review developers' employment/consulting contracts and job descriptions – Was work in the course of employment? Is assignment language broad enough?
 - Are there any records of where development took place – i.e., at the office or at home?
 - Review developers notes

Typical IT Transactional Due Diligence



- Copyrights

- How to determine whether the target owns them?
 - Search registers by jurisdiction
 - Software
 - Is there any open source code and if so, is the target in compliance with the applicable licenses?
 - NDAs/Non-competition agreements
 - Any security interests or assignments?

Typical IT Transactional Due Diligence



- Other Registrable IP
 - Trade-marks, integrated circuit topographies, industrial designs
 - Search various registers by jurisdiction
 - Check for proper ownership, assignments, security interests
 - Length of registrations, maintenance fees
 - Any security interests?
 - For trade-marks, “common law” searches may also be advisable
 - Business names; domain names

Typical IT Transactional Due Diligence



- Compile unregistered IP assets
 - Trade secrets, know-how, common law trademarks, unregistered trade names, trade dress, and unregistered copyrights, etc.
 - Inventor/author, uses, and dates of first use should be identified
 - Have trade secrets and know-how been protected by non-disclosure agreements?

Typical IT Transactional Due Diligence



- **Compile unregistered IP assets**
 - Examine all IP-related agreements such as licenses
 - Are licenses in good standing and fees paid? Are licenses subject to transfer restrictions?
 - Any SRED credits owing?
 - Obtain reps and warranties concerning any known or potential issues

IT Due Diligence – Tips



- Focus on what is relevant
 - Make sure you understand the company's history, products and plans
 - Make sure you understand the relevance of the IT system(s) to the transaction or other purpose of the diligence exercise – are they relevant at all?

IT Due Diligence – Tips



- **Plan ahead**
 - Don't rely on precedents – draft a diligence questionnaire that is specific to the purpose at hand
 - Try to ask questions that will elicit useful responses for further diligence purposes

IT Due Diligence – Tips



- Do not take anything at face value – additional verification efforts could include:
 - Search registries whenever possible; manual searches sometimes uncover database errors
 - Examination and analysis of search results
 - Verifying unregistered IP rights

IT Due Diligence – Tips



- Do not take anything at face value – additional verification efforts could include:
 - Review of licenses, development agreements, etc.
 - Personal interviews with staff and former staff
 - Review and analysis of potentially infringing claims

IT Due Diligence – Tips



- Do not take anything at face value – additional verification efforts could include:
 - If the IT assets are located in foreign jurisdictions, do local laws create any unforeseen issues?
 - IT due diligence may be an iterative process

IT Due Diligence – Tips



- Do not take anything at face value – additional verification efforts could include:
 - Don't despair at problems that due diligence uncovers - discrepancies uncovered through due diligence might be fixed through “work-arounds”

IT Due Diligence



THANK YOU FOR YOUR ATTENTION!

Bernice Karn
Cassels Brock & Blackwell LLP
40 King Street West
Toronto, Ontario
M5H 3C2
416-869-5721
bkarn@casselsbrock.com



www.casselsbrock.com

2100 Scotia Plaza, 40 King Street West, Toronto, Canada M5H 3C2 Phone 416 869 5300
© 2007–2009 Cassels Brock & Blackwell LLP. Cassels Brock and the CB logo are registered trade-marks of Cassels Brock & Blackwell LLP.
™ Trade-mark of Cassels Brock & Blackwell LLP. All rights reserved.