Proposal Document: Global Investment Banking Analytic Services

Date: June 13, 2006

Presented to:

Karen Jim
Merrill Lynch
Contract Specialist

karen_jim@ml.com
T. 609 274 7797
F. 609 274 0439

Submitted by:

Anmol Bhandari
Vice President, Business Development
Copal Partners

anmol_bhandari@copalpartners.com
T. 646 361 9599
F. 646 390 3491

Approved by:

Rishi Khosla
CEO
Copal Partners

rishi_khosla@copalpartners.com
T. 646 662 4260
F. 646 390 3491

TABLE OF CONTENTS

APPENDIX

Executive Summary

As the leading provider of outsourced investment banking research and analytics, Copal Partners is pleased to participate in Merrill Lynch's RFP process.

Copal is a firm of over 350 professionals, based in New York, London, and Delhi, specializing in products geared towards bulge bracket, multi-national investment banks. We are the only firm that has managed to significantly scale an outsourced investment banking relationship and reengineer banking processes. Through this experience comes knowledge and expertise in completing the products outlined in the RFP SOW. Our experience with investment banks also allows us to provide significant value-add with regards to process improvement within our client's organization. We have engaged our clients in a number of efficiency improving initiatives, including, creating comps databases and profile automation engines. In addition, Copal's investment banking focus means that we understand the need for client confidentiality, and as such, maintain one of the most stringent compliance policies in the industry.

Through sourcing the brightest talent in the industry (over 88% of employees are advanced degree holders), implementing best-of-breed methodologies and processes, and offering a near turn-key solution, we can provide Merrill Lynch with a seamless transition onto our outsourcing platform along with unsurpassed quality. Copal's obsession with quality is grounded in its proprietary processes which consist of focused training, multiple quality-check layers, and detailed methodology documents. In addition, we are uniquely able to provide added confidence to our clients through the robust auditability features in all of our products. Every delivery by Copal features scanned mark-ups of the source documents used, as well as comments in excel cells detailing information such as the source used, page number, and pro forma treatments for a particular number. These extra steps provide added transparency and have proven to be vital in building confidence with our clients.

A key feature of Copal's offering is the speed of implementation and ease of workflow management. Within seven days Merrill Lynch can be running on Copal's outsourcing platform, and this includes the execution of highly customized products. Initiating work is as simple as contacting our NY-based Engagement Manager who liaises with our workflow desk and execution teams in India. Copal allows bankers the flexibility of contacting the execution team in India directly with questions, or their NY-based engagement manager 24x7, providing unparalleled client support. Our deep expertise in investment banking support allows us to do this with minimal effort on the part of Merrill Lynch.

In summary Copal Partners:

- is at the forefront of the investment banking outsourcing space; we are the largest provider of investment banking services;
- is the only research provider in India who has successfully scaled an investment banking outsourcing relationship; and

- even when considering captive units, is the only player who has reengineered investment banking output production

In addition, our commitment to the community makes us a truly unique partner in the outsourcing industry, we:

- organize food distribution on a weekly basis to poor people in Delhi;
- have launched an initiative to produce institutional quality research on charities in India. Charities will be rated and covered on a quarterly basis, essentially to ensure funds are diverted to the most effective and sustainable charitable organizations;
- regularly donate to charitable organizations in the health sector; and
- regularly raise funds to help provide for the impoverished citizens of our community

We look forward to continuing through the Merrill Lynch RFP process, the terms of which we would fully comply with. We strongly believe that our wealth of experience and best of class offerings make us the ideal provider of outsourced services for Merrill Lynch Investment Banking.

Yours faithfully,

Rishi Khosla
Chief Executive Officer
Copal Partners

Company Overview

About Copal Partners

Copal Partners is a research and analytics company serving clients in the Financial Services industry. Our clients include several of the leading bulge bracket investment banks, mid-size advisory firms, financial sponsors and hedge funds. We are currently the largest outsourced financial research provider, with over 350 employees in New York, London and Delhi. Our Knowledge Center and research teams are based in Delhi. Copal is BS 7799 certified and compliant, reflecting our heavy focus on information security and confidentiality.

Though we maintain a diverse client base, Copal is focused primarily on providing bulge bracket and boutique investment banks research and analytics services with unparalleled quality, flexibility, and transparency. We are the preeminent provider of outsourced investment banking services, with more than 80% of our revenue coming from that one area.

Our largest client, a bulge bracket investment bank, is a prime example of our capabilities in the investment banking space. At inception, Copal Partners began working with a single industry group within this client. Today we serve this same client with a team of approximately 200 professionals, supporting the pitch process and mandated deals. Through the pitch process we are responsible for creating the content behind entire pitch books including target/buyer lists, trading and transaction comparables, and accretion/dilution modeling. We support mandated deals with similar functions including work on Information Memorandums and modeling support.

Our non-executive directors include:

- Andrew J. Melnick - Former Global Co-Head of Investment Research at Goldman Sachs (Member of Goldman Sachs' Executive Management Committee) and Head of Research at Merrill Lynch

- Sir Sushil Wadhwani - Former member of the Monetary Policy Committee at the Bank of England and Head of Equity Strategy at Goldman Sachs

Financial Strength

Copal is a privately held company. We are in the processes of filing for an initial public offering on the London AIM exchange in Q4 2006; Deutsche Bank and KBC Peel Hunt have been engaged to act as the Company's advisors. Our accounting advisors are currently KPMG.

Copal Partners has been profitable since its inception in 2002. Our current revenue run rate is over $10 million. Our current cash balance is over $2 million and we plan to strengthen our cash position with the initial public offering in Q4 2006.

Breadth of Capabilities

Copal provides an array of products and services that are customizable for each individual client based on specific methods, templates and formats. A key differentiator of Copal's services is the transparency it offers through audibility features such as marked scanned source documents, and commented excel cells. For example, each figure in a trading comps analysis would include a commented cell that provides information on the source type (e.g. 10K, 10Q), source date, source page number, and details on pro forma treatments. Additionally, the relevant pages from the source documents would be marked, scanned, and included in the delivery of the comps. If a figure provided by Copal Partners is ever questioned, the banker can quickly and easily trace the number to its source. This avoids the need for multiple iterations, and as a result the research outsourcing process is significantly more efficient. The audibility of Copal's work is a key feature that gives clients a high degree of confidence in Copal output.

Copal Partners continues to successfully build on its four areas of expertise. Within each vertical Copal has managed to consistently outperform client expectations.

The four practice areas of Copal are as follows:

- **Investment Banking (80% of revenue):**
  Copal provides support for pitch and mandated work for leading bulge bracket investment banks as well as mid-size advisory firms. Products include: comparable company analysis, precedent transaction analysis, company profiles, pro-forma merger models, industry analysis, buyer/target lists and library services
- **Credit Research (15% of revenue):**
  Copal works for several credit/distressed debt hedge funds. Products include: capital structure & debt covenants analysis, risk exposure, business analysis, bankruptcy analysis and credit reports
- **Equity Research (<5% of revenue):**
  Copal supports equity research divisions of bulge bracket firms as well as independent research houses. Products include: valuation models, sector/ thematic research, company studies and summary research products
- **Strategy & Consulting (<5% of revenue):**
  Copal works with consulting firms, corporations and private equity firms. Products include: industry studies, competition analysis, industry profit/value chain analysis, consolidation analysis and SWOT analysis

Section 2.0 Management Proposal

Section 2.1 Implementation/Transition Plan

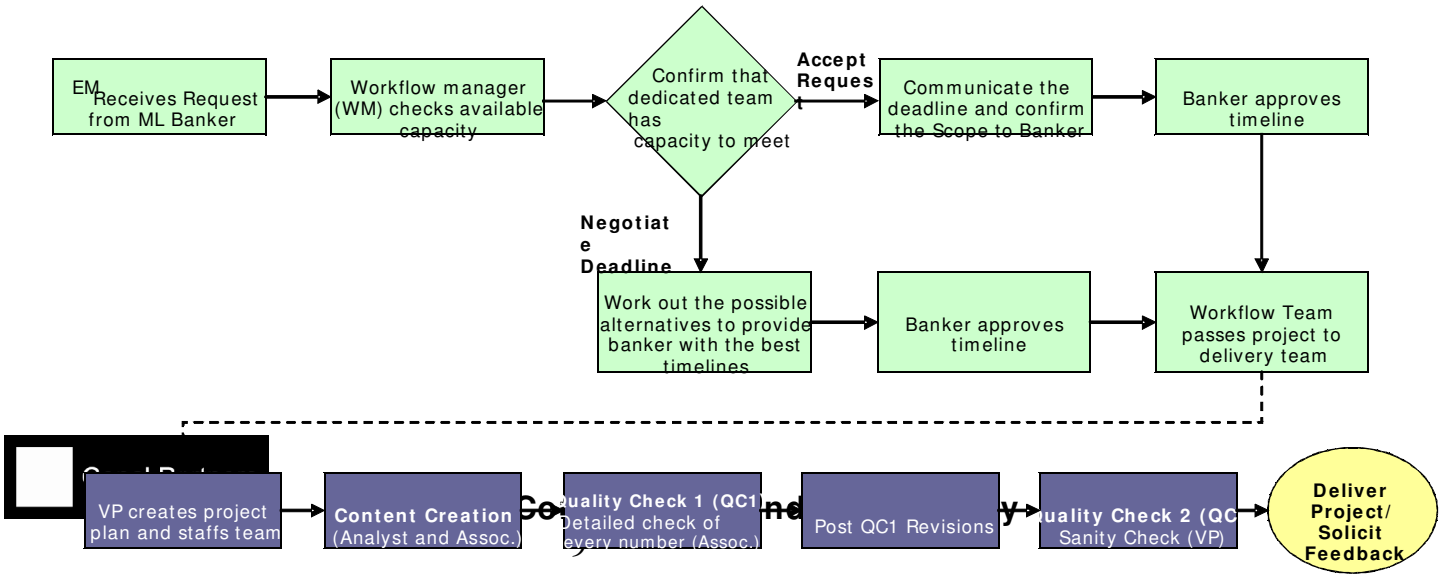
With our deep experience in investment banking methodologies, Copal Partners can provide a seamless transition to our outsourced solution. Within 1 week, Copal Partners can assemble a dedicated team, and begin fielding project requests from Merrill Lynch bankers. Through the workflow we receive from Merrill Lynch our teams will document methodology and create banker and industry specific templates for each product. Below we describe our implementation, and workflow plans in detail:

2.1 (i) Workflow

One of the largest difficulties in servicing investment banks is the volatility and short deadlines that characterize workflow. We have spent a significant amount of time developing expertise in optimizing capacity and making resources fungible to deliver large amounts of work against stringent timelines. Copal Partners' proprietary workflow methodologies allow clients to seamlessly integrate onto our outsourcing platform. Through the combination of a NY-based engagement manager (EM), as well as a 24x7 workflow desk in India, Merrill Lynch can easily and efficiently initiate, amend, and take delivery of projects.

Merrill Lynch will have a NY-based EM that will serve as the primary local contact for its bankers. All new project requests by bankers are either initiated by an email to a Merrill Lynch-dedicated secure mailbox or by telephone to the EM. The Engagement Manager liaises with the workflow desk in India to assess time estimates for the project, current available capacity of the dedicated team, and estimated delivery schedule based upon the bankers deadline. The project details are then communicated to the banker and the project is started upon banker approval.

During the course of the project the banker may communicate additional details or changes by contacting either the Engagement Manager or the team in India. In addition, if Copal requires any further clarifications, the dedicated Copal VP will contact the banker directly via email or through a scheduled telephone call. Based on client preference, delivery of projects can either be by email, secure FTP, or a dedicated network connection.



2.1 (ii) Proposed Organizational Chart

The organizational chart below shows the proposed Merrill Lynch team, as well as key support and management personnel.

Note: Orange boxes reflect delivery staff dedicated to Merrill Lynch. In addition to the staff shown above, Copal's delivery organization includes over 350 people supporting investment banking, equity research, credit research, hedge fund, private equity and corporate clients

2.1 (iii) Scheduling

Standard hours for Copal's project delivery teams in India are 9:30am to 7pm local time
(12:00am EDT to 9:30am EDT), Monday through Friday. However, the delivery team generally works banking hours, including late nights and weekends as necessary.

2.1 (iv) Timeline

Given its deep experience and expertise in investment banking outputs, Copal Partners offers a turn-key solution which allows investment banking clients to leverage Copal's outsourcing capabilities virtually immediately. Through its talented pool of employees, Copal can assemble a dedicated team of 20-30 professional within a 1 week period. The dedicated team will spend five to seven days training on Merrill Lynch specific methods, templates, and formats as based on the examples provided in this RFP. Post this initial period the team will continually develop a set of industry and banker specific methodology documents that outline the processes and methods used for each research/pitch product in detail. These methodology documents are shared with Merrill Lynch bankers and are implemented upon approval. Within seven days, Copal Partners can begin executing projects as defined per the SOW (comps, profiles, risk report cards, etc).

Once Merrill Lynch bankers start sending work requests, we would create methodology / process documents for all outputs. These would be approved by Merrill Lynch and teams would be further trained on these.

2.1 (v) Management Backgrounds: On/Off Site (London, New York, Delhi)

Rishi Khosla
CEO (London/New York)
Rishi Khosla is CEO and one of the Founders of Copal Partners. His primary responsibilities are overseeing the company's global business development activities. Previously, he managed the private equity and venture capital activities of Lakshmi N. Mittal, the global steel entrepreneur who was ranked the 3rd richest individual globally behind Bill Gates and Warren Buffet. His 1999 tech vintage

venture portfolio has realized a 4.6x capital return including two billion dollar enterprises – PayPal and IndiaBulls. Prior to managing Mr. Mittal's portfolio, he was in the business development team at GE Capital, reporting to the President of GE Capital Europe. During his tenure he attained approval from Jack Welch to establish an early stage venture fund for GE Capital, which he co-managed. Rishi started his career in banking where he wrote one of the first equity research notes on the third generation of mobile telephony, and participated in a number of advisory transactions, including an asset swap between GRE and ING and a divestment program for the Polish government. Rishi is a Board Member of TiE UK. He holds a bachelors degree in Economics from the University College London, and a masters in Accounting and Finance from the London School of Economics where he was awarded a scholarship by the Economic and Social Research Council.

Joel Perlman
President (London/Delhi)
Joel Perlman is President and one of the Founders of Copal Partners. He manages the global service delivery activities of the firm. Previously, he founded and managed Latin Venture, a marketing firm with operations in the US and major Latin American markets. Latin Venture was sold to a WPP sponsored venture capital fund, where Joel joined as Managing Partner. Joel also assisted startups Zumba Productions and Comerxia in achieving profitability and entering international markets. Previously, he was a consultant at McKinsey & Company, where he participated in several engagements with Fortune 100 companies, with emphasis on business strategy, growth and process reengineering in the banking industry. Joel is an advisor to CarullaVivero, the largest food retailer in Colombia with over USD 1 billion in sales. He has an undergraduate degree with honors in Finance and Philosophy from Georgetown University and a masters in Accounting and Finance from the London School of Economics.

Aman Chowdhury
Country Head (Delhi)
Aman spent six years at JPMorgan, most recently as Vice President and Head of FIG at JPMorgan's captive investment banking research unit in Mumbai. Previously, he spent 4 years in JPMorgan's Investment Banking group in New York participating on a range of M&A and corporate finance transactions. Prior to JPMorgan, Aman has worked in the Investment Banking divisions of CSFB in New York and Lazard in Delhi. Aman has an MBA from Darden Business School (University of Virginia) and an undergraduate degree in Economics from St. Stephen's College (University of Delhi). Aman is also a CFA charter holder.

Anmol Bhandari
Vice President Business Development (New York)
Anmol worked with Goldman Sachs in their Hedge Fund Strategies Group (HFS) in Princeton, New Jersey. Anmol was a member of the risk and quantitative strategy team that focused on absolute return investment strategies within both sector-specific and multi-strategy funds. The group was one of the first to offer manager-of-manager hedge fund strategies and manages over $8 billion in assets. Previously, Anmol worked with Donaldson Lufkin & Jenrette, in the prime brokerage

team, focusing on high net worth individuals. Anmol holds a bachelors degree in Electrical Engineering from Villanova University.

Employee Backgrounds: Delivery Teams (Delhi, India)

Copal focuses heavily on recruiting and retaining the highest quality individuals. Most of Copal's professionals are Masters degree holders or Chartered Accountants.

Copal's on site teams are composed of VPs, Associates and Analysts. Their typical backgrounds are:

Vice President

- 5-10 years of experience in Investment Banking, Investment Research, Consulting or Industry
- Leading school Masters and/or CA
- Chartered Accountant Certification

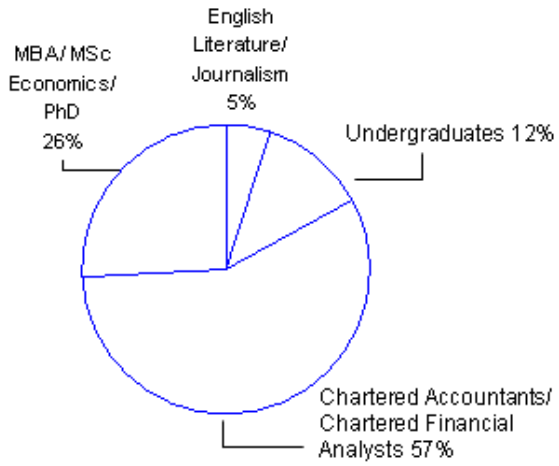
Associate

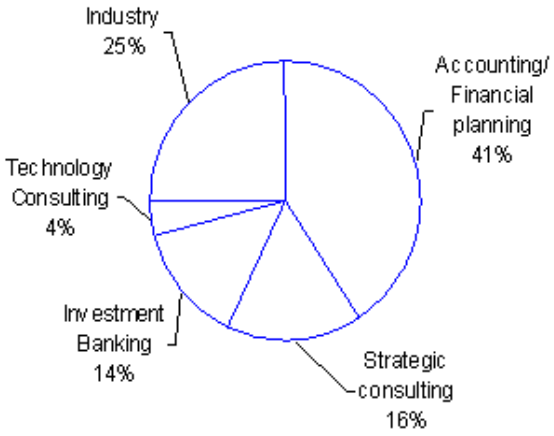
- 2-5 years of experience in Investment Banking, Investment Research, Consulting or Industry
- Leading school Masters and/or CA
- Chartered Accountant Certification

Analyst

- Masters from a leading school
- Chartered Accountant Certification

Below is a graphical depiction of Copal's on site employee's backgrounds:





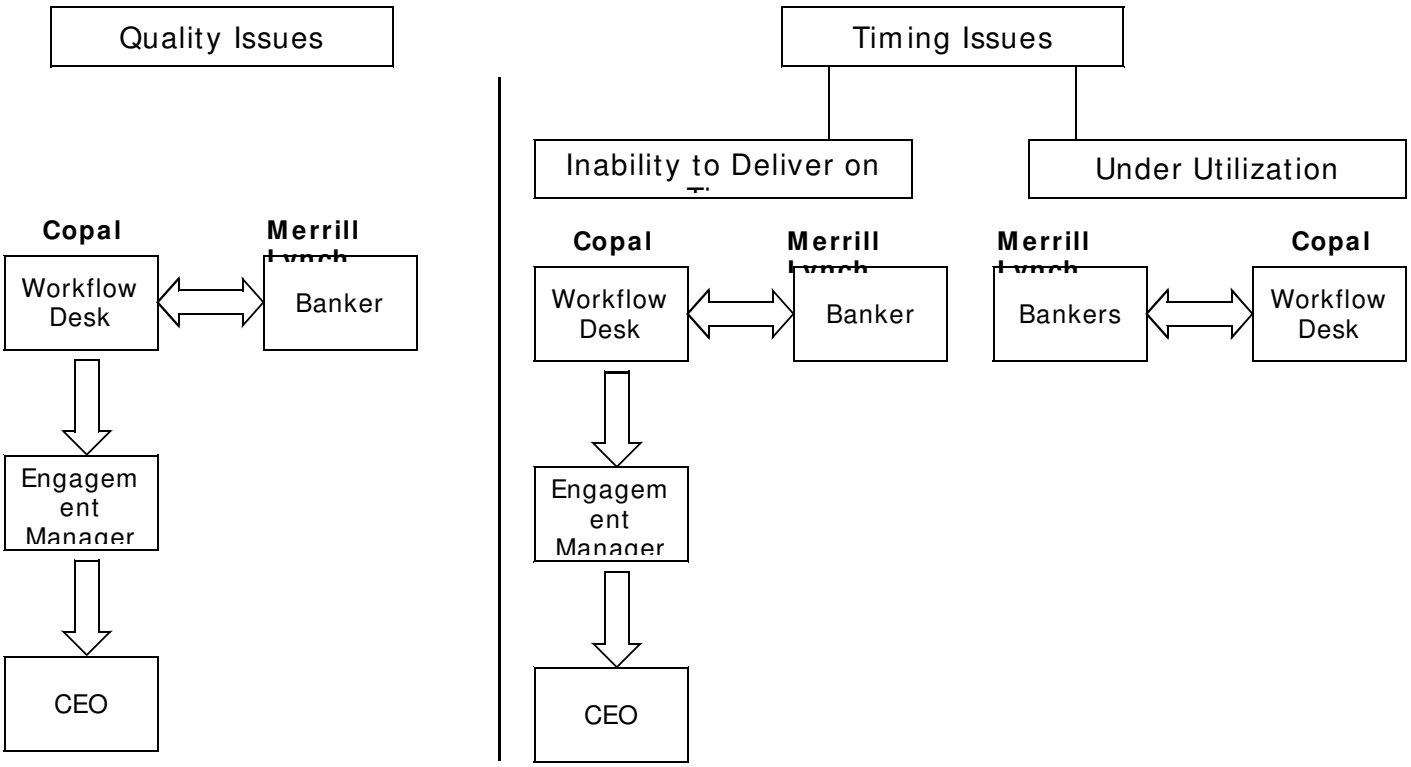
2.1 (vi) Conflict Resolution

Copal's service policy is to resolve all apparent problems in the shortest feasible time frame given that the vast majority of the work undertaken by Copal is time critical. Given Copal's 24x7 client support structure, all client issues are actioned immediately and almost always resolved within 24 hours, if not sooner.

Should there ever be any quality and or delivery issues with the work delivered, the Merrill Lynch Banker can directly contact the New York-based Engagement Manager, India Workflow desk, and / or the delivery teams. Should there be any issues, the workflow team would escalate the issue to the Engagement Manager and ultimately to the CEO if required.

At any given point if there is excess capacity within the ML team, the workflow desk would follow up with the bankers directly to notify them of the available capacity.

Below is a depiction of our escalation procedure.



2.1 (vii) Training/Recruiting & Scale

Training

All employees go through a four week training that mirrors associate and analyst training programs conducted at Wall Street firms. Two weeks are spent in general training (e.g., finance, accounting, valuation, and firm-wide topics such as compliance and confidentiality). In the second half of training, new employees participate in product specific training (e.g. banking, credit research, etc). Below are example pages from the comps modules we use in our training sessions. Our modules are comprehensive, covering everything from a conceptual lesson on enterprise value, to execution instructions directing analysts which sources to use and how to get them.

Copal Partners

Enterprise Value

Formula to calculate Enterprise Value

Market Capitalization
+
Total Debt
+
Minority Interest
+
Preferred Stock
+
Capital Leases
-
Cash & Cash Equivalents
=
Enterprise Value or "EV"

Total Enterprise Value (TEV or EV) is the term bankers use when they refer to the total value of a company (also referred to as Aggregate Value)

Enterprise value is a measure of the actual economic value of a company at a given point of time. It reflects what it would actually cost to purchase the entire company

One could believe that a possible way to calculate the value of a company would be to look at the value of the assets in the company's balance sheet. This is a common misconception because the assets in the balance sheet are recorded using the historical value and thus it is not the value the company has today

Generally for public companies TEV = market value of the equity + total debt (short and long term) + minority interest + preferred stock + capital leases – cash and cash equivalents

The method and assumptions for calculation of enterprise value varies with every financial institution, banker and industry

Copal Partners

Definitions

Market capitalization	▪ Represents the market value of all outstanding shares ▪ Calculated as Total number of shares outstanding x current share price
Stock Options	▪ A privilege, in which the underlier is the common stock of a corporation, that gives the buyer the right, but not the obligation, to buy or sell a stock at an agreed-upon price during a certain period of time or on a specific date ▪ A right granted to employees of a company to buy a certain amount of shares in the company at a predetermined price. Employees typically must wait a specified vesting period before being allowed to exercise the option
Warrants	▪ A derivative security or certificate that gives the holder/ bearer the right to purchase securities (usually equity) from the issuer at a specific price within a certain time frame
Convertibles	▪ Securities, usually bonds or preferred shares, that can be converted into common stock at a specified conversion price

Copal Partners

Definitions

Fully Diluted shares	▪ Represents the number of shares that would result if all stock options, warrants and convertible debts were traded in for stock. ▪ Treasury stock method is used in determining the number of shares outstanding ▪ Results in an increased number of shares outstanding and decreased earnings per share
Treasury stock method	▪ The purpose of the Treasury method is to account for the cash generated by the exercise of options and/or warrants ▪ Treasury stock method assumes that the options and/or warrants are exercised at the beginning of the year (or issue date if later) and such proceeds are used to repurchase outstanding shares of common stock ▪ Example

Current share price	$ 50
Shares outstanding	400 mn
Options/ warrants outstanding	10 mn
Exercise price	$ 25
Proceeds from conversion of in the money options	10 x $ 25 = $ 250mn
Stock buyback (at premium)	$ 250 / $ 50 = 5 mn
Diluted Shares	400 + 10 – 5 = 405 mn

▪ The comps template is formulated to apply this methodology

Copal Partners

Definitions

Total debt	▪ Includes all interest bearing obligations both long-term and short-term such as loans, credit facilities etc ▪ Excludes in-the-money convertible debt
Minority Interest	▪ Represents portion of equity not owned by the majority shareholder - a significant but non-controlling interest of less than 50%
Preferred equity	▪ Represents class of stock carrying preference over equity stake holders to receive dividend and repayments in the event of liquidation
Capital lease	▪ A lease that transfers substantially all risks and rewards of ownership to the lessee
Cash and cash equivalents	▪ Represents cash, marketable securities and short-term investments that can easily be converted to cash

Recruiting

Copal Partners retains some of the brightest individuals in the industry, approximately 88% of our employees are post-graduate degree holders or

Chartered Accountants/Chartered Financial Analysts. Our senior employees typically have experience in Investment Banking, Investment Research, Consulting and Industry.

Our recruiting strategy varies by employee level:

- At the junior level, Analysts are recruited through specialized HR consultants in India who help us source talented individuals with relevant experience. In addition, we participate in campus recruiting at tier 1 and 2 schools.
- At the senior level, for associates and VPs, recruiting is generally conducted through internal employee references and specialized HR consultants. These employees are required to have highly specialized skills, therefore we take additional care to verify that we are targeting the correct individuals.

We are currently set-up to be able to hire and train 25-50 people per month on an ongoing basis.

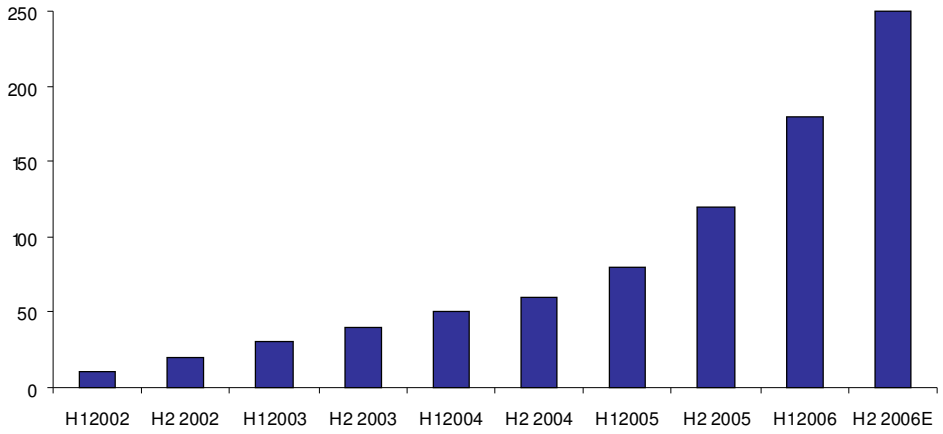
Scale

Given the flexibility requirement of our clients, it is crucial for our organization be able to seamlessly scale its operations without adversely impacting the quality of the output. Copal not only recognizes this fact, but has several proprietary operational processes in place to ensure that it remains the industry best practice.

First, the creation of detailed methodology documents allows for efficient replication of products and processes; the process of bringing new resources up the learning curve is greatly diminished. Second, the ability to quickly secure talented resources allows us to rapidly scale our teams. Finally, our focused and effective training methods allow our new employees to be effective contributors from the very beginning, enabling us to have a strong pipeline for additional capacity at all times.

We are the only outsourcing firm to have successfully demonstrated the ability to scale for an investment banking client. In the case of our largest client, we began with a team of 10 professionals in 2002 and have since grown to 200 professionals.

Copal Partners - Proven Ability to Scale with an Investment Banking Client
Headcount Growth of Larget Client



Proven Ability to Scale, A Case Study:

Our largest client, a multi-national, bulge-bracket investment bank, began working with us in 2003. In the past three years, we have successfully scaled the relationship to over 200 dedicated personnel for this single client. Throughout the relationship, not only have we added significant resource flexibility, but we also added value through reengineering several of their processes. The latter has resulted in significant internal efficiency gains for our client. Our client has also been able to significantly improve junior banker lifestyle through this initiative.

The relationship began with 10 people in 2003 and was limited to us performing company profiles and trading comps. The confidence our client had in our work product grew quickly, generating increased demand and an increased team size to service it. Soon, we were adding more client industry groups to our platform, and adding 10 to 20 new people per month to the team. Moreover, we increased the scope of our services, performing research and analysis throughout their value chain up to mandated deal work. A key to the client's rapid adoption of our services was the transparency we provided in each of our products. By providing easy auditablity features such as marked source documents, and source information for every number in our financial analysis, outsourcing to India became less of a "black box" and resulted in immediate confidence in the integrity of the output. The impact of integrating Copal into our client's workflow has been significant; for example we maintain over 2,500 trading comps centrally, and our client has planned to reduce new junior banker going forward.

2.1 (viii) Parallel Services

Per client confidentiality agreements, Copal does not disclose client names. Copal does however support investment banking divisions similar to Merrill Lynch in size and prominence in the US, Europe and Asia.

2.1 (ix) Related Production Services

Copal Partners has two related production services divisions:

- **Business Information Services (BIS)** – Our Business Information Services group provides essential investment banking library services to our clients. We possess a large selection of subscription services and databases, and trained experts that excel at locating and delivering highly relevant research to bankers. Example services include: primary research, secondary research, company filings, tear sheets, Bloomberg data, Factiva news runs, and Thomson Deals/SDC data.
- **Desktop Publishing (DTP)** – Our highly skilled DTP professionals provide formatting support for all content in Microsoft Word and PowerPoint. DTP gives Copal the ability to deliver products (e.g. comps, profiles, industry studies) that are fully formatted and conform to Merrill Lynch's design template. As a result, upon delivery a banker is only required to insert the Copal pages into the final pitch book.

Section 2.2 Subcontractor Listings

Copal Partners does not plan to engage any subcontractors with regards to this RFP. Copal will use its own offshore center in India for the delivery of services contemplated in this RFP.

Section 2.3 Disaster Recovery

Disaster Recovery

Copal has two operating facilities in Northern India and each facility serves as a warm-standby DR site for the other. All company data is mirrored in real time between the facilities, and is also stored on tape in a secured third-party facility. In the event of a partial or total system outage in any one of the facilities, appropriate personnel are alerted via a call tree, and sent to the backup site. Each site contains sufficient workspace and PCs to support operations at a minimum of 20% capacity. The PCs are preconfigured and on-line, and teams can be operational within 4 hours of failure. Each DR area has the same security and compliance controls (access controlled rooms, shredders, VLANS, etc) and the same support equipment (data sources, scanners, printers).

Our disaster recovery plan was last tested in Q1 2006. Additionally, we expect a dedicated DR operating facility to be operational by Q4 2006.

Business Continuity/Resumption Plans

Copal's data processing and delivery systems are redundant at every level to ensure uninterrupted service. Each data service has local and remote-site mirror servers to ensure that the company is impervious to system crashes. Every site has multiple connections to the internet, which flow through redundant layer-3 switches and firewalls.
In the event of a catastrophic disaster, teams can be relocated to the secondary site and make immediate use of hot-standby servers, printers, scanners, data services and desktops. 20% of the total team can be fully operational from the secondary site within 4 hours of a disaster.

Section 2.4 Quality Control (QC) / Quality Assurance (QA) / Client Satisfaction/Document Quality Assessment

Our quality management process relies on 5 key elements:

1. **Training**: Our training program, modeled on Wall Street training programs, provides our teams with highly relevant classroom and on-the-job training. The training program takes our personnel through key concepts and real-life exercises.
2. **Methodology Documents**: we build methodology documents for all of our products. These methodology documents provide a detailed review of how to build the products, including sources and process. This allows us to institutionalize knowledge and ensure consistent high quality.
3. **Quality control processes:** integrity of the data is the most critical part of our work product. Before a delivery goes out, the Associate will check every single number against the actual source. The VP will also conduct sanity checks, and in case an outlier is found, the team will re-run the analysis
4. **Auditability:** we make our work fully auditable for clients. With every delivery, we attach scanned backup materials. This provides comfort to our clients as they can easily audit numbers/details back to filings/source documents.
5. **Feedback:** We solicit feedback ratings scores from bankers on all of our deliveries in each of the following areas: adherence to agreed deadline, accuracy of work, adherence to scope, and communication clarity. Bankers rate the deliveries from 1 to 5, 1 being poor, and 5 being very good. This feedback is communicated to the teams and incorporated in the relevant methodology documents when appropriate. On average, feedback scores have been between 4 and 5. Should any score fall below 4, the Merrill Lynch workflow team would immediately follow up with the bankers to work through any issues with the delivery.

Moreover, overall performance is measured on an ongoing basis. In addition to informal feedback sessions on a regular basis given by their managers, employees receive 2 formal reviews during the year. Performance reviews are based on a detailed and comprehensive performance tracking system, in which the employee

is rated on a number of hard and soft parameters. We categorize each employee into 3 groups and provide strong career and financial incentives for performers in the highest group. Performers in the lowest group, which constitute approximately 15% of the workforce, are given a formal warning, and managed out of the firm if performance does not improve within the stipulated timeframes. We consistently benchmark performance across the firm to use best-in-class methodologies, and deploy them across the firm.

Through our MIS system, we carefully track and measure performance against client and internal KPIs, including: deadline adherence, mechanical errors, understanding of GAAP/IFRS regulations, generation of new ideas, spelling/grammar errors, content consistency, terminology and style, correct format, effective communication/analyst interaction, invoice timeliness, invoice accuracy, and prompt issue resolution.

Should document quality not meet the client's established acceptable level, we implement an escalation process to ensure a high degree of customer satisfaction. Copal's service policy is to resolve all apparent problems in the shortest feasible time frame.

Section 2.5 Cost Reduction

In working with our existing investment banking clients, Copal Partners has successfully identified and implemented meaningful improvements in operating efficiency. To date, these efforts have reduced duplicative efforts and rework among client Investment Banking teams. As an example, a Copal-initiated program for one client resulted in the creation of a database of trading and transaction comp analyses and profiles across specific industry teams globally. This avoids the current situation within investment banks where companies may be comped by different teams in different regions many times within the same week. It also avoids profiles continually being recreated.

Copal would suggest implementing a similar procedure to centralize trading and transaction comps across Merrill Lynch, and set up weekly trading comp database deliverables to the team to ensure that comps are always updated and minimizing rework across client groups. In addition to the database effort for comps, Copal will also build and maintain an ongoing profiles database to ensure that there is minimal rework. Benefits not only include a reduction in duplication and rework, but also shorter turn-around time, as Merrill Lynch bankers would now have access to updated comps and profiles on a utility basis as opposed to a request-based basis.

Section 2.6 Performance Guarantee/Contract Compliance

Performance Guarantee
Copal Partners maintains the highest standards of quality, timeliness and availability to its clients. We are confident in guaranteeing a performance consistent with the Illustration of Outputs (Appendix C) and SOW provided by Merrill Lynch.

Specific guarantees such as turnaround time of outputs, quality, time to acknowledge receipt of requests and issue resolution are amongst the service levels that will be monitored and put in place with the Merrill Lynch team. Each deliverable is independently reviewed via banker questionnaires and feedback reports. We will maintain a high level of quality per key performance indicator as agreed with Merrill Lynch. The workflow team maintains the key performance indicators (KPI's) on a daily basis. The KPI report will be distributed on a weekly basis for Merrill Lynch's review and service credits will be applied should criteria not be kept.

User feedback

We measure customer satisfaction at the project-specific and client engagement levels. At the project-specific level, we measure customer satisfaction based on a 1-5 scale that clients use to rate a number of project criteria, including: timeliness of delivery, accuracy of work, adherence to scope, and communication clarity. We believe that this simple and quick feedback process works best given the limited time our clients typically have. Our average score across clients is between 4 and 5 (Satisfied and Very satisfied). At the client engagement level, we conduct client engagement feedback reviews and go into depth on client's experiences. These are periodic meetings in which the project-specific feedback is reviewed, and additional discussions regarding general or recurring feedback are addressed.

Service Level Agreements (SLA's)

To ensure consistency in timeliness and quality of deliverables, Copal Partners will put in place and be measured against the following SLA's:

1. Deadline adherence
2. Mechanical Errors
3. Generation of new ideas
4. Spelling/Grammar Errors
5. Content Consistency
6. Terminology and Style
7. Correct Format
8. Effective Communication/Analyst Interaction
9. Accurate MIS
10. Prompt issue resolutions

Compliance

Copal Partners is able to maintain confidentiality through strict internal compliance requirements which all employees are trained on. We have a dedicated Head of Compliance, and a Compliance department which focuses solely on maintaining our best-of-breed compliance standards. Our compliance department conducts training, monitors locations, and sees that all business activity falls within Copal's compliance standards.

All employees are required on commencement of employment to sign a personal declaration acknowledging receipt of the compliance manual and undertaking to

observe both the spirit and the letter of its principles, procedures, rules and regulations in their entirety.

In order to protect from unwarranted risk, all employees are required to immediately notify the Compliance Department of any personal or financial changes that may affect their ability to carry out their duties in a professional manner.

The Compliance Department will be notified of any domestic, personal or business relationship between employees. Each situation is reviewed on an individual basis taking into consideration risk posed to the client and its employees.

During employment including during any period of paid leave, no employee may directly or indirectly be engaged in any business, trade or occupation than that of Copal Partners. In addition, there is a restriction of owning more than a 1% of the issued shares or securities of any companies which are listed.

Through our compliance training, all employees understand the fact that insider dealing is a criminal offences, prohibited under various acts. At the commencement of employment all employees are required to provide a detailed list of all securities they own as well as an official latest quarterly summary security report provided by their brokerage firms. To buy or sell shares, all employees must obtain clearance and written authorization from the Compliance department.

All information is treated as confidential and or commercially sensitive. All employees are required to sign Confidentiality agreements whereby they shall not at any time either during employment or after its termination, for whatever reason, use, communicate or reveal to any person any information concerning Copal Partners and its clients.

All teams work from dedicated rooms with their own printing and shredding facilities. Access in and out the team rooms is controlled by electronic photo ID cards, based on two secure access doors. Information is only allowed to be shared on a need-to-know basis. No confidential or client information can be removed from the dedicated rooms at any time, either physically or electronically. Employees are not allowed to bring in or remove any writeable media devices (e.g. disks, CD's, USB storage keys). All papers are shredded using the dedicated facilities.

Our detailed compliance manual is included in the Appendix F.

Section 2.7 Billing

Billing

Each deliverable is classified according to the specific team, location and or cost center. The billing process is based upon these unique project codes to facilitate transparency. The unique codes can be broken out and designated as per Merrill Lynch's internal requirements. For example, MLN001, would be a code for Merrill Lynch (ML), New York (N), project code 1 (001).

Copal Partners will bill on the last day of each month for all work completed in the current month. Copal supports EDI billing, in addition to hard copy billing.

Management reports are generated on a daily basis. The workflow desk tracks projects from initiation through completion. At the initiation of a project, the workflow desk confers with the VP to estimate the capacity requirement of a new project and to block capacity appropriately. At the completion of a project, the VP confirms actual time taken for the project.

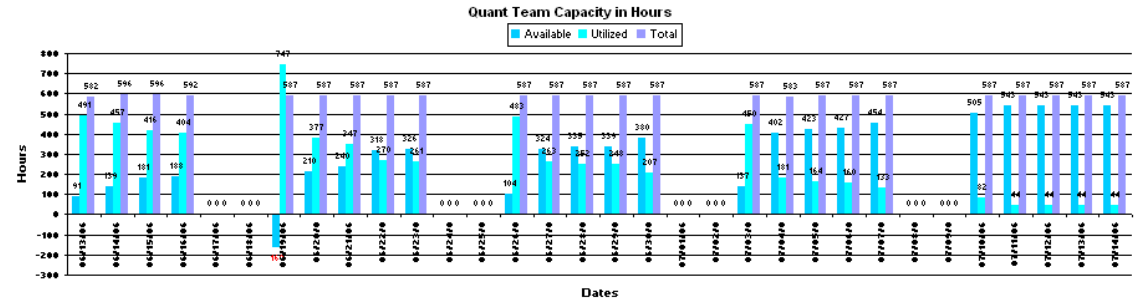
We maintain historical information in our records for a mutually agreed period of time. This information can be extracted, on demand, at relatively short notice or as Merrill Lynch requires.

Section 2.8 Reports

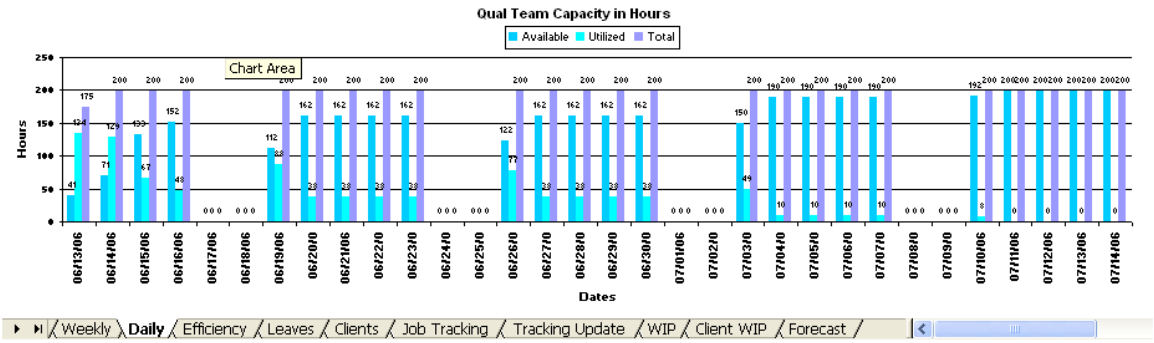
Reporting

Copal Partners will provide Merrill Lynch with comprehensive reporting on a regular, and as needed basis. Reporting will include monthly staff turnover, variance in cost from previous month, QC%, feedback scores, and other related reports In addition, Copal will provide the following reports:

- Capacity Tracker – The capacity tracker is a dynamic tool that calculates the total available capacity based on such factors as employee efficiencies, work product hours and total available efficiency. The charts below depict a capacity snapshot for a given period as well as employee efficiency chart used to calculate capacity.



* Hours have been divided in the ratio 3:1 for Quant:Qual



DO NOT ADD OR DELETE ROWS AND COLUMNS. To add a team member just input the name, designation and efficiency levels in the appropriate place

Employee Code	Analyst	Designation	Team	Profiles	Profiles QC	ECM weekly	ECM weekly QC	Daily News	Daily News QC	Memos	Memos QC	Product 2	Product 2 QC	QUAL AD Hoc	QUAL AD Hoc QC	Comps	Comps QC	Benchmarking	Benchmarking QC	Financials	Financials QC	Memos Financials	Memos Financials QC	Precedent Transactions	Precedent Transactions QC	Quant Ad Hoc	Quant Ad Hoc QC
25341	Abey Mittal	Senior Analyst	QC													35%											
25062	Abhas George	Associate	QC														65%										
25405	Abhishek Islam	Associate	QC													35%		35%									
25007	Ainul Agarwal	Senior Associate	QC														100%		100%				100%	100%			
25147	Ajaya Singh	Senior Analyst	QC													80%		80%									
25389	Akhil Mishra	Senior Analyst	QC													40%		35%									
25274	Aman Behera	Senior Analyst	QC													60%		55%									
25392	Amresh Goel	Senior Analyst	QC													40%		40%									
25008	Anish Tiwari	AVP	QC														100%		100%				100%		100%		
25061	Ankur Bhardwanju	Associate	QC														75%		75%				75%		60%		
25414	Ankur Jain	Senior Analyst	QC													35%		30%									
25251	Anuj Kumar Singh	Senior Analyst	QC													55%		55%									
25176	Ashish Patel	Senior Analyst	QC													60%		60%									
25385	Ashish Gupta	Senior Analyst	QC													40%		40%									
25318	Ashish Patel	Senior Analyst	QC													55%		50%									
25434	Ashok Manchandani	Senior Analyst	QC													25%		20%									
25387	Ashu Arora	Senior Analyst	QC													40%		40%									
25179	Atul Bansal	Senior Analyst	QC													75%		75%									
25133	Babneet Rawal	Associate	QC														60%		60%								
25299	Bharat Kukreja	Senior Analyst	QC													60%		60%									
25297	Chanchal Saini	Senior Analyst	QC													60%		60%									
25383	Chetan Kumar	Senior Analyst	QC													40%		40%									
25390	Debasish Mohapal	Associate	QC													40%		40%									
25413	Devender Dangri	Senior Analyst	QC													35%		30%									
25336	Dheeraj Mahal	Associate	QC													40%		40%									
25154	Dinesh Jindal	Senior Analyst	QC														55%		55%								
25258	Dinesh Dhariwal	Senior Analyst	QC													75%		70%									
25187	Gaurav Gupta	Senior Analyst	QC													80%		80%									
25433	Harsh Sharma	Senior Analyst	QC													25%		20%									
25367	Hitesh Chawla	Associate	QC													55%		45%									
25139	Jitender Arora	Senior Analyst	QC													80%		80%									
25259	Jitesh Datt	Senior Analyst	QC													75%		70%									
25162	Kamlesh Sharma	Senior Analyst	QC													75%		75%									

Total / Weekly / Daily / **Efficiency** / Leaves / Clients / Job Tracking / Tracking Update / WIP / Client WIP / 4cast /

- **Work in Progress Report** – The Work in Progress Report is the snapshot of any outstanding projects to date. The sheet provides a static view of all the requests still to be delivered. The WIP is maintained by the workflow teams and is delivered each morning to the client, and relevant Copal Engagement Managers and VPs.

Copal Partners

Project Code	Product	Description	Client	Deadline Date	Day	Time	Zone	Vice President	Forecasted Hours	Hours Left
MLU227	Comps	Internet Comps Database (23)	Tim	24-Jan-06	Tuesday			Colin Adler	17	17
MLN276	Daily News	DITM 23rd - 27th Jan 2006 & Weekly Deals Overview - New York FSG	Kenneth	27-Jan-06	Friday			Ashish Mclaren	20	20
MLN275	Daily News	DITM 23rd - 27th Jan 2006 - New York	Michael	27-Jan-06	Friday	9:00	EST	Ashish Mclaren	25	25
MLN274	Memos	Briefing Memos Database (21)	Alexander	27-Jan-06	Friday			Ashish Mclaren	147	147
MLN273	Comps	Weekly Comparable Company Updates... Student Lending Industry	Evelyn	23-Jan-06	Monday			Colin Adler	3	3
MLN272	Memos	Six Briefing Memos... Woodward Governor, Xerox, Encana	Philip	1-Feb-06	Wednesday			Ashish Mclaren	150	128
MLN259	Comps	Sixty Nine Comps with Extended Financials and LTMs... Entergy Corp, FPL Group, Cin	Ruth	6-Feb-06	Monday			Colin Adler	621	558
MLI1291	Daily News	DITM 23rd - 27th Jan, 2006 - London	Craig	27-Jan-06	Friday	8:15	GMT	Ashish Mclaren	25	25
MLI1290	Profiles	Seven Profiles... TJ Maxx, Poundstretcher, Ethel	Satya	24-Jan-06	Tuesday			Ashish Mclaren	49	49
MLI1289	Comps	Ten Comps... Carrefour, Casino, Delhaize	Guillaume	23-Jan-06	Monday			Colin Adler	35	35
MLI1288	Precedent Transactions	Eleven Precedent Transactions... Tata tear The Tetley Group	Guillaume	28-Jan-06	Saturday			Colin Adler	41	37
MLI1287	Precedent Transactions	Precedent Transactions Database	Himanshu	27-Jan-06	Friday			Colin Adler	113	98
MLI1286	Comps	Comps Database Update (232)	Clara	30-Jan-06	Monday			Colin Adler	233	233
MLI1285	Comps	Weekly Comparable Company Updates	Gunhild	23-Jan-06	Monday			Colin Adler	19	19
MLI1284	ECM weekly	Weekly News Update	Michael	23-Jan-06	Monday			Ashish Mclaren	8	8
MLI1283	ECM weekly	ABB/IPO Database	Michael	23-Jan-06	Monday			Ashish Mclaren	4	4
MLI1282	ECM weekly	Blocktrade Database	Michael	23-Jan-06	Monday			Ashish Mclaren	4	4
MLI1281	ECM weekly	Weekly Deal Database	Michael	23-Jan-06	Monday			Ashish Mclaren	8	8
MLI1274	Benchmarking	Sixty Two Comps with Benchmarking and LTMs...Amcor, Crown, Rexam	Michael	TBD				Colin Adler	744	744
MLI1273	Comps	Nineteen Comps... Manpower, Robert Half, Kelly	Philipp	24-Jan-06	Tuesday	9:00	GMT	Colin Adler	57	34
MLI1271	Benchmarking	Five Comps with Benchmarking... Ducati, KTM, Harley-Davidson	Carl	24-Jan-06	Tuesday			Colin Adler	60	57
MLI1270	Comps	Seventeen Comps with Extended Financials... ABP, Forth Ports, PD Ports	Jasvinder	25-Jan-06	Wednesday			Colin Adler	85	68
MLI1258	Benchmarking	Sixty Eight Companies Benchmarking ... Metals & Mining Comps Database	Tzveta	23-Jan-06	Monday			Colin Adler	248	198
MLI1253	Comps	FIG Comps Database (162)	Anneke	23-Jan-06	Monday			Colin Adler	150	120
MLI1252	Comps	Metals & Mining Comps Database (75)	Pierre	23-Jan-06	Monday			Colin Adler	204	91
MLI1251	Comps	Steel Comps Database (40)	Pierre	23-Jan-06	Monday			Colin Adler	40	28
MLC017	Comps	Energy Trusts Comps Database (14)	Eitan	25-Jan-06	Wednesday			Colin Adler	11	11
MLB114	QUAL AD Hoc	Technology Newsletter	Kenneth	28-Jan-06	Saturday			Ashish Mclaren	10	10
MLB112	Comps	Comps Database Update (433)	Tucker	27-Jan-06	Friday			Colin Adler	325	325
MLB111	Comps	Comps Database Update (37)	Shamit	27-Jan-06	Friday			Colin Adler	28	28
MLB110	Comps	Comps Database Update (34)	Neeraj	25-Jan-06	Wednesday			Colin Adler	34	34
MLT761	Product 2	Eleven Profiles & Fifty Two Precedent Transactions... Avaya, Mitel, 3Com	Mark	24-Jan-06	Tuesday			Ashish Mclaren	217	217
MLT759	Comps	Semiconductor Comps Database (195)	Kirtan	30-Jan-06	Monday			Colin Adler	146	146
MLT755	Comps	Eleven Comps... Emap, Lagardere, Mondarori	Vicky	23-Jan-06	Monday	8:00	GMT	Colin Adler	33	26

- **Engagement Tracker** – The Engagement Tracker sheet is a summary sheet for any given period that lists the pertinent details relative to a single project. Each project entry contains a description of the project, the request and delivery dates, the individual responsible for its delivery, the cost, time spent and feedback.

Copal Partners

Engagement Reference	Engagement Type	Project Name	Engagement Description	CAG Team	MD/ Director/ VP
ML091	Two Detailed Profiles... DibCom, Integrant (DR)	Technology	Six Companies Consensus Estimates...Philips, Micron, Freescale (DR)	Technology	Ben McMillan
ML090	Benchmarking Seven Companies... Avaya, Intertel, Aspect (DR)	Jacobi	Two Detailed Profiles... DibCom, Integrant (DR)	Technology	Ben McMillan
ML089	Industry Thematics & One Detailed Profile... Frontier Silicon (DR)	Technology	Benchmarking Seven Companies... Avaya, Intertel, Aspect (DR)	Technology	Seth Wootherspoon
ML088	Twenty Five Thumbnails... Video Conferencing Sector (DR)	Technology	Industry Thematics & One Detailed Profile... Frontier Silicon (DR)	Technology	Jim Lee
ML087		Technology	Twenty Five Thumbnails... Video Conferencing Sector (DR)	Technology	Michael Connolly

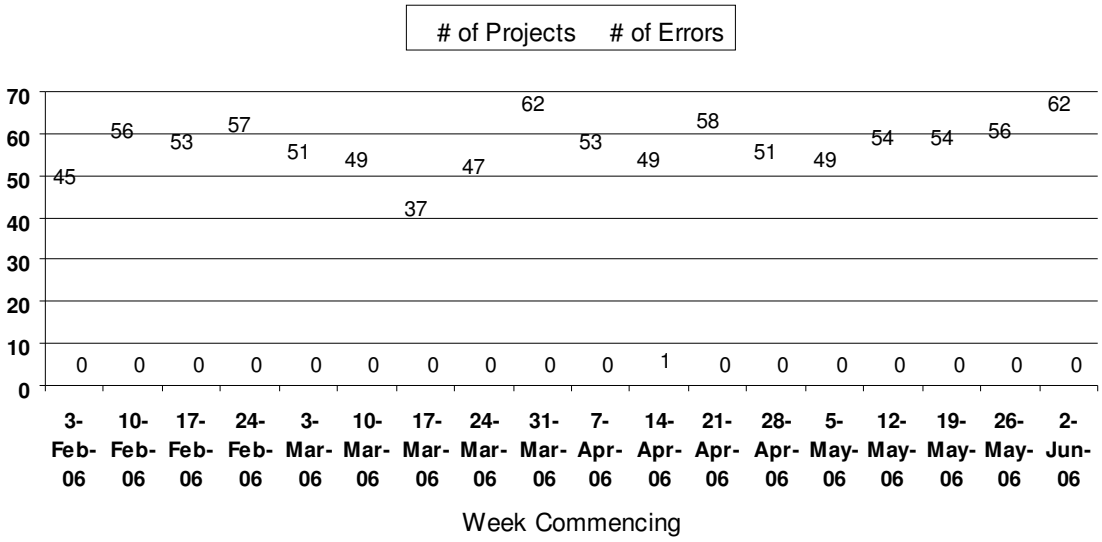
Team	Request Date	Deadline	Delivery Date	Copal Team		# Estimat	# Actual	# Hours	Sources (GBP)	Commercials (GBP)	Score (1-5)	Explanation
Associate/ Analyst				EM	Team Lead							
Arbinda Singh	7-Jun-06	13-Jun-06	WIP	Anmol Bhandari	Vimal Kumar	30		30	TBD			
Carl O' Donnell	6-Jun-06	7-Jun-06	7-Jun-06	Anmol Bhandari	Ankur Malhotra		15	15	1 Alacra report			
Arbinda Singh	5-Jun-06	7-Jun-06	7-Jun-06	Anmol Bhandari	Vimal Kumar		70	70	0			
Louis Russo	2-Jun-06	3-Jun-06	3-Jun-06	Anmol Bhandari	Ankur Malhotra		18	18	1 Alacra report			
Louis Russo	2-Jun-06	3-Jun-06	3-Jun-06	Anmol Bhandari	Ankur Malhotra		19	19	0			

- **Feedback Tracker** – The Feedback Tracker tracks the average response of the feedback from the bankers.

Client Feedback Summary

Team	Total Responses	Timeliness of delivery	Accuracy of work	Adherence to scope	Communication clarity	Overall Score
Quant	54	4.70	4.22	4.56	4.50	4.52
Qual	50	4.64	4.24	4.45	4.44	4.44
Quant & Qual	9	5.00	4.67	4.56	4.89	4.78
Summary	113	4.70	4.31	4.52	4.50	4.51

- **QC Tracker** – The Quality Control Tracker shows a visual depiction within a given timeframe of the errors made amongst deliverables



- **Staff Breakdown Tracker** – The Staff Breakdown Tracker tracks the mix of staff members across time

Section 2.9 Technology/Technology Security

Technology Configuration (PC)
Our standard PC configuration is a P4 of 2.6-3.0 GHz, with 256 MB RAM, 40GB HDD, and Windows XP SP2. While we find this configuration provides suitable performance for the services that our clients require, we would be able to comply with Merrill's stated requirements.

Technology Security

Please refer to our response to 2.11 below

Section 2.10 Client Listing

As the leading provider of outsourced financial research, our clients are many of the premier global financial institutions, including bulge bracket investment banks, equity research department of bulge bracket banks, hedge funds, private equity firms and independent equity research firms. We are the only outsourcing provider to focus primarily in the investment banking space, with over 80% of our revenue coming from that one area. It is a testament to our strong investment banking work flow processes, and superior output quality that we are the only firm to successfully scale an investment banking relationship.

Section 2.11 Physical/Information Security

Copal Partners maintains the highest standards for both physical and information security. Copal manages security according to a BS7799-certified information security management system (ISMS), which includes stringent controls on electronic and physical transmission of all client-specific information. We rely on redundant, state-of-the-art firewall technology to secure our information systems and employ round the clock security personnel and access-controlled rooms to maintain physical security. A strictly enforced compliance effort also helps maintain high standards of information security. As per our own firm policy, Copal Partners would not process or store any personal information about Merrill Lynch clients or employees.
Copal Partners would not process or store any personal information about Merrill Lynch clients or employees; with regard to other sensitive data, Copal manages security according to a BS7799-certified information security management system (ISMS).

Network security controls include Cisco ASA firewalls, HP filtering routers, antivirus gateways and multiple dedicated VLANs for partitioning sensitive data to access-controlled segments of the network. Each dedicated VLAN has its own domain, file, and antivirus servers. Network and server engineers are on-site 24x7. Employees are electronically prohibited from accessing Webmail sites or from sending mail to any address outside the organization, except where required for business purposes.

Our network is secured from intrusion via redundant Cisco ASA firewalls, and further secured by HP Procurve filtering L3 switches. Dedicated client systems and servers are segregated into protected VLANS and communication across these VLANS is electronically prohibited.

To ensure physical security, Copal's sites are manned by security guards 24x7. Access to any area within the facility requires an electronic access card when entering or leaving. Client teams work in dedicated, access-controlled rooms. Access to the delivery areas requires two separate levels of card access. Each room has its own printing, scanning, and shredding facilities, and clean desk and shredding policies are strictly enforced.

Regulatory compliance includes a trade authorization system to protect against insider trading. All employees must request authorization before making a trade on any foreign or domestic security. All employees are required to report all trading accounts, and submit statements of trades and holdings on a quarterly basis to reconcile trades and authorizations.

To ensure compliance, access, server, and network logs are all reviewed daily for unusual events. Evidences of process adherence are collected and reviewed weekly, and a complete internal ISMS audit is performed twice yearly. Employees attend compliance training during induction, and refresher sessions are held quarterly for all employees.

Section 2.12 Miscellaneous

Exceptions to the RFP Requirements

Copal Partners agrees to meet all requirements of the RFP and has found no exceptions to the RFP Requirement.

Contact Persons

Rishi Khosla – CEO
33 Glasshouse Street
London, W1B 5DG
T: 646-662-4260
F: 646-390-3491
rishi_khosla@copalpartners.com

Anmol Bhandari - VP, Business Development
350 Park Avenue, 5th Floor
New York, NY 10022
T: 646-361-9599
F: 646-390-3491
anmol_bhandari@copalpartners.com

References

The references below have performed similar type of work as outlined in the RFP, and may be contacted by Merrill Lynch:

Daniel Marovitz
Chief Strategy Officer
Deutsche Bank, International Banking Division
Winchester House
1 Great Winchester House
London EC2N 2DB
Tel: +44 20 7545 8000

Jan Metzger
Director, Credit Suisse
Credit Suisse Investment Banking
One Cabot Square
London E14 4QJ
Tel: +44 20 7888 8888

Victoria Coles
COO, Lazard Investment Banking Europe
50 Stratton Street
London W1J 8LL
Tel: +44 20 7187 2808

Build-Operate-Transfer

Copal is prepared to offer Merrill Lynch 3 non-traditional operating options:

1. **Build-Operate-Transfer** – Copal would build and manage a dedicated team either out of Copal's center in Delhi, or an Indian location of Merrill Lynch's choice. Copal would develop the team for a mutually agreed timeframe, at which point Merrill Lynch would have the option to buy out the dedicated team, or retain Copal to manage and grow the team.
2. **Joint-Venture** – Copal would create NewCo, a Merrill-Copal joint-venture company consisting of Merrill's dedicated outsourcing team. Merrill Lynch would have full governance rights in the entity including a board position and full information rights.
3. **Commitment based Warrants** – Based on revenue commitments by Merrill Lynch, Copal would offer warrants on the equity of Copal Partners. The warrants would be exercisable after a predefined period, and would grant Merrill Lynch an equity stake in Copal Partners.

Management Proposal Questionnaire

Question 1: Do you currently offer an offshore provider who could provide these services?

Copal Partners is the offshore provider that would provide all the services described in the Merrill Lynch Statement of Work.

We maintain a team of over 350 professionals in Delhi, India that provide our clients with outsourced research and analytics solutions. We were founded in 2002, and are the only outsourcing provider to focus almost exclusively on investment banking clients. In addition, we are the only firm (third-party, or captive) to successfully scale an investment banking relationship; our largest client currently has 200 dedicated members.

Our proprietary workflow model, ability to source the brightest talent in the industry, and unmatched work quality makes us the preeminent investment banking outsourcing partner.

Question 2: Please name the offshore provider(s) you currently work with, and state its size and base location of operations.

Our outsourcing office is based in Delhi, India and we source all our research internally. We currently have over 350 professionals that provide financial research and analytics services to investment banking, hedge fund, private equity and corporate clients.

Question 3: What commercial arrangement do you have with this vendor(s)?

The outsourcing facility in Delhi, India is wholly-owned and operated by Copal Partners.

Question 4: How long has this collaboration been in place?

Not applicable

Question 5: Which other clients do you have that utilize an offshore solution? Please name them and briefly describe the current solution, including a staff overview and type of work undertaken.

Copal Partners has a number of leading investment banks and hedge funds as clients. As per client non-disclosure agreements, Copal cannot release the name of individual clients. However, Copal does work with firms similar to Merrill Lynch in size and function. For these clients, Copal maintains dedicated teams that perform company profiles, trading comps, transaction comps, benchmarking analysis, sector overviews, industry thematic research, valuation modeling, and accretion/dilution modeling.

Our dedicated investment banking teams are staffed similar to Wall Street firms, with VPs, Associates and Analysts. VPs typically have masters degrees (MBA/Masters in Finance) from top-tier universities and at least 5 years of experience in the financial research industry. Associates also have masters degrees from top programs, and have 2 to 5 years of relevant experience. Analysts are typically from top-tier undergraduate institutions, and have 1 to 2 years of financial analysis experience.

Question 6: What technology would Merrill Lynch need to facilitate this solution?

None; all implementation is conducted internally. Copal offers a virtually plug-and-play solution, whereby almost all implementation time and resource investment is absorbed by us.
For a longer term relationship it may be beneficial for both parties to implement a dedicated lease line between our facilities and Merrill Lynch's network.

Question 7: If your solution does not involve 100% of the work being taken offshore, please describe how you propose to interface with the offshore resources.

Our proposals assume 100% of the work is conducted offshore in India. However there will be a NY based Engagement Manager.

The NY-based Engagement Manager acts as both a relationship manager for Merrill Lynch bankers, and a liaison with our workflow desk in India. The Engagement Manager will most often be the first point of contact for project intake.

Question 8: Please provide a listing of all languages (and dialects) supported at offshore locations.

Copal Partners possess a talented and diverse workforce that has proficiency in English, Hindi, Spanish and a number of Indian local languages.

Section 3.0 Scope of Work and Performance Standards

Section 3.1 Planning and Service Scope of Work

Services

Initial Services- Pilot

Copal Partners understands the pilot will be for an initial period of 3-4 months and will comprise of 20-30 personnel working for ML groups globally.

Rollout of Services- Rollout

Copal Partners understands the rollout will be for a one-year period and comprise of 60-100 personnel working for ML groups globally. The contract will be negotiated on an annual basis. Merrill Lynch shall have the ability to cancel the Rollout without penalty upon 60 day written notification.

Vendor Resources

Copal Partners offers a turn-key solution whereby Merrill Lynch will not have responsibility for management, scheduling, training, costs, or any other human resources related activities. We source the best talent in the industry, and would be happy to share with Merrill Lynch the qualifications of the members staffed on its dedicated team for pre-approval.

Copal Partners uses the same market data as used by most Wall Street investment banks; we do not have requirements for special resources. Merrill Lynch can engage Copal Partners in one of two models for market data:

1. Merrill Lynch can provide Copal Partners with a pass-through license to leverage Merrill's internal resources
2. Copal Partners can procure commercially available databases (e.g. Bloomberg, Reuters, Thomson's Financial, Factiva, etc) and charge Merrill Lynch for source costs.

Copal Partners does not require dedicated resources from Merrill Lynch to execute any of the outsourcing initiatives outlined in the RFP. Copal would only require a primary relationship contact who can aid with issue escalation. We typically coordinate directly with our client team's staffers.

Please see section 2.1 for details on the recommended workflow. Our workflow methodologies have been developed by working with bulge bracket global investment banks for over three years. We are the only research outsourcing provider focusing almost exclusively on investment banking outsourcing, and as a result, we are able to leverage years of relevant experience to provide Merrill with a best-in-class offering.

Service Levels

Copal Partners has SLA's (service level agreements) and KPI's (key performance indicators) in place with several clients.

To ensure the quality of output for Merrill Lynch deliverables, we propose to put similar guidelines in place.

Copal Partners would take each key performance indicator (KPI) and apply minimum/target performance standards against them. The performance standards would then roll into service credits back to Merrill Lynch if performance is missed.

An integral part of the Merrill Lynch and Copal relationship will be based upon the feedback and management reporting system. Copal would issue a monthly KPI/SLA report to Merrill Lynch as shown below. Copal is open to modification of the KPI's and or creation of new standards as per Merrill Lynch's requirements.

The time period for the minimum acceptable performance and target performance is per calendar month, unless state otherwise.

Definitions of the terms used in the table are as follows:

- 'Performance Factors' represent broad categories against which Copal is measured
- 'KPI's' describe the method by which Copal is measured
- 'Minimum Acceptable Performance' is the low-end benchmark. Service Credits will apply for performance below this level.
- 'Target Performance' represents the standard that Copal Partners should routinely deliver day after day

Performance Factors	KPI	Minimum Acceptable Performance	Target Performance	Service Credit
Output Quality				
Timeliness	The proportion of jobs that are completed by the agreed deadline (timescales are set out in the table "Average Cycle Times For Standard Requests")	TBD	TBD	TBD
Accurate Response	The number of jobs that are completed in accordance with the Banker's request.	TBD	TBD	TBD
Completeness	The number of jobs that are completed without any relevant information missing (eg files, reports, lists etc). Each piece of missing information shall be counted as 1 error.	TBD	TBD	TBD

Duplicated Or Redundant Information	The number of jobs that are completed without - 1) Any duplication of any information 2) Any information submitted that was not requested 3) Any information that is not in English (or any other language pre-agreed with the requestor) Each occurrence of the above shall be counted as 1 error.	
Correct Format	The number of jobs that are completed in the agreed format without any deviations	
Data Integrity	The number of jobs that are submitted that cannot be 'opened'/ read or have corrupted / missing data content (due to Copal Partners error). Each corrupt file shall be counted as 1 error.	

Supporting Services & Infrastructure				
Communication link	The amount of downtime due to fault that is Copal Partnerss responsibility.	TBD	TBD	TBD
Resource Numbers Compliance	The variation in the actual number of resource days provided from the required number of resource days (including satisfying requirements for additional resources in accordance with the Volume Change Mechanism). Performance shall be measured annually on the basis of each resource working 48 weeks per year.	TBD	TBD	TBD
MI Reporting Timeliness	The number of occasions that the Management Information Report has not been completed by required deadline.	TBD	TBD	TBD
MI Reporting Accuracy	The number of errors in any Management Information reporting for KPI's and PI's. An error is the monthly value for any KPI or PI missing or incorrect [any errors to be corrected within 30 days of detection].	TBD	TBD	TBD
Issue Resolution	The elapsed time from notification, to resolve any errors of the types described under "Output Quality" above.	TBD	TBD	TBD

Compliance & Legal				
Confidential Information Management	The number of events of non-compliance with requirements	TBD	TBD	TBD

Scope Policing	Performance of any work by Copal Partners that is knowingly outside of the agreed documented scope of the services.	TBD	TBD	TBD
Workflow	Performance of the work in accordance with agreed workflow procedures.	TBD	TBD	TBD

Training/Recruitment/Retention

A. Recruitment and Training of Staff

Copal Partners is committed to recruiting and developing the highest quality individuals. With its emphasis on professional development, Copal has consistently outperformed the industry in employee retention.

Approximately 88% of our employees are post-graduate degree holders or Chartered Accountants/Chartered Financial Analysts. Copal hires first-attempt Chartered Accountants and MBAs from Tier 1/2 schools at the junior levels and Tier 1/2 schools at the mid/senior levels. Our senior employees typically have experience in Investment Banking, Investment Research, Consulting and Industry.

Our recruiting strategy involves developing partnerships with HR consultants who help source qualified candidates. Our resource needs extend beyond campus recruiting, and we are very active in the lateral market. We are currently set-up to be able to recruit and train 25-50 people a month on an ongoing basis.

All employees go through a four week training that mirrors associate and analyst training programs conducted at Wall Street firms. Two weeks are spent in general training (e.g., finance, accounting, valuation, and firm-wide topics such as compliance and confidentiality). In the second half of training, new employees participate in product specific training (e.g. banking, equity research, credit research, etc).

B. Employee Retention Statistics

The statistics below represent the historical turnover rates for the past 6 months, 1 year and 2 years. Due to the nature of the industry as a whole, we expect attrition rates to be around 30%, yet have been able to keep them under 20% as employee retention has been strong.

Much of our attrition (i.e. “Left the Industry” and “Other”) is rooted to personal situations with employees, mainly family moves, marriages and or other personal events. Aside from personal reasons, attrition can be attributed to those individuals at very junior levels that are still exploring career options.

Below are our employee retention statistics.

	Last 6 months	Last 1 year	Last 2 years
Left for a competitor	11	12	16
Left the industry	22	26	32
Terminated	11	18	28
Promoted/Transfers	41	61	75
Other	7	7	8

C. Retention Strategy

Copal Partners succeeds at maintaining retention rates above the industry average by offering career development, training and incentives. We provide employees with concrete career plans, and detailed metrics to achieve them. This transparency enables employees to take a long term view. We also offer ongoing professional development opportunities and invest heavily in the training of our employees. At the early stages of their careers, training is focused on technical skills; in the middle stages of their careers, training is focused on managerial skills; in the latter stages of their career training is focused on client management skills. Our technical training is modeled on the training provided by major investment banks to the clients. Our managerial and client management training borrows from the training principles of top consulting companies. Overall, we provide rare development and training opportunities that would be challenging for our employees to find elsewhere.

As importantly, if not more so, we offer our employees generous monetary incentives. While our employees make competitive salaries, the bonus component we provide is higher than the industry average and is heavily differentiated based on performance. As a result, our employees are strongly incented to work towards the bonus, and perform at very high levels.

Finally, we foster a collegial culture that makes Copal Partners a truly unique place for our employees. We sponsor a host of activities aimed at fostering strong personal and professional bonds between our employees. We find that these events have a direct effect on employee satisfaction, and as result, drive productivity and retention. For example, one of the activities is the Copal Partners Food Drive, where every week groups of Copal employees deliver hot food dishes to local Delhi citizens in need. Other activities include: regular contests, team outings, and company offsites.

D. Merrill Lynch Training

Copal Partners would not require any Merrill Lynch led training to deliver the specified outputs. We would request VBA Macros that Merrill Lynch uses internally for presentations, as well as any related training material.

Travel Policy

Copal employees will have the flexibility to travel as required by the client in the most cost effective manner.

Holiday Schedule

Copal Partners understands the nature of the Investment Banking industry and the required services. Copal possesses the flexibility to provide coverage to Merrill Lynch 365 days a year.

Pricing

RESOURCE TYPE DEFINITIONS

Copal shall provide resources to perform the services in accordance with the definitions set out in the table below -

Type	Minimum Education	Minimum Relevant Work Experience	Key Responsibilities / Rationale	Core Skills
Engagement Manager	**Masters** /MBA /CA from a top tier University	**5 years** in financial services research including 3 years managerial experience	Client relationship management ; monitoring of performance in accordance with key high level objectives; continuous improvement ; service development in accordance with changes in requirements ; high-level performance issues resolution	Outsourced service management / organization; relationship management; motivation and mentoring; strong spoken and written English; performance optimization; strong financial research services process knowledge
Vice President	**Masters** /MBA/ CA from a top tier University	**5 years** in financial services research role	Ensuring operational / "day to day" delivery of service in accordance with requirements; operational issues resolution; operational relationship management and ongoing user feedback; responsibility for quality compliance of work submitted; coaching and team motivation	Team management experience; performance management; process improvement / troubleshooting; motivation and mentoring; strong client focused interpersonal skills; time management and deadline adherence; strong financial research process / operational knowledge
Senior Associate	**Masters** /MBA/ CA from a top tier University	**4 years** in financial services research role	Responsible for performing research and analysis work ; coaching / mentoring and quality checking the work of junior colleagues	Highly numerate; highly analytical; business awareness; good spoken and written English; Desktop PC Skills (Word, Excel, PowerPoint), time management / deadline achievement; coaching / mentoring
Associate	**Masters** /MBA/ CA from a top tier University	**2 year** in financial services research role.	Responsible for performing research and analysis work ; coaching / mentoring and quality checking the work of junior colleagues	Highly numerate; highly analytical; business awareness; good spoken and written English; Desktop PC Skills (Word, Excel, PowerPoint); time management / deadline achievement
Senior Analysts	**CA/Bachelors** degree from a top tier University	**2 years** in financial services research role.	Responsible for performing research and analysis work including quality checking the work of junior colleagues	Highly numerate; highly analytical; business awareness; good spoken and written English ; Desktop PC Skills (Word, Excel, PowerPoint)

Analysts	**Bachelors** degree from a top tier University	**0-1 year** in financial services research role.	Responsible for performing research and analysis work	Highly numerate; highly analytical; business awareness; good spoken and written English; Desktop PC Skills (Word, Excel, PowerPoint)

Commercial Structure for Pilot Project

The pilot program is for a 3-4 month period with a team size of 26 individuals. All costs are indicated as per annum. Therefore the cost of the pilot stage would be $263,250 based on a team of 26 people over 3 months.

Pilot-Offshore (India)							
Merrill Lynch Investment Banking Pilot Pricing Sheet - ANNUAL PRICING	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Total**
Resources							
Staff Title	EM	VP/AVP	Senior Associate	Associate	Senior Analyst	Analyst	0
Total Resources	1	2	2	5	12	4	26
Direct Costs - Annual							
Compensation							
Base Salary	$ 44,772	$ 74,000	$ 40,000	$ 67,500	$ 108,000	$ 32,200	$ 366,472
Benefits	$ 677	$ 3,000	$ 3,000	$ 7,500	$ 18,000	$ 6,000	$ 38,177
Overtime	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Bonus	$ 4,043	$ 14,800	$ 8,000	$ 13,500	$ 21,600	$ 6,440	$ 68,383
Contingent Salaries	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Other Non-Compensation							
Communications & Technology	$ 1,355	$ 6,000	$ 6,000	$ 15,000	$ 36,000	$ 12,000	$ 76,355
Occupancy	$ 3,161	$ 14,000	$ 14,000	$ 35,000	$ 84,000	$ 28,000	$ 178,161
Other (please describe)	$ 1,806	$ 8,000	$ 8,000	$ 20,000	$ 48,000	$ 16,000	$ 101,806
Total Direct Costs	$ 55,813	$ 119,800	$ 79,000	$ 158,500	$ 315,600	$ 100,640	$ 829,353
Management Fee (as necessary)	$ 7,056	$ 33,544	$ 22,120	$ 44,380	$ 88,368	$ 28,179	$ 223,647
Pass-through One-Time Costs (please describe) [1]						$ 10,000	
Pass-through Recurring Costs (please describe) [2]							$ -
Total Billing Amount - ANNUAL	**$ 62,869**	**$ 153,344**	**$ 101,120**	**$ 202,880**	**$ 403,968**	**$ 128,819**	**$ 1,053,000**

Note:
All costs are per annum
[1] Pass through one time cost is 10,000 USD as a setup of the dedicated infrastructure for the Merrill Lynch teams
[2] We would suggest Copal leverages from Merrill Lynch's existing market data service contracts, and therefore would not expect a pass through cost

Commercial Structure for Rollout of Services

The initial service rollout period is for 1 year with a team size of 82 individuals. All costs are indicated as per annum.

Rollout -Offshore (India)							
Merrill Lynch Investment Banking Rollout Pricing Sh	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Global Banking Analytic Services**	**Total**
Resources							
Staff Title	EM	VP/AVP	Senior Associate	Associate	Senior Analyst	Analyst	0
Total Resources	2	5	6	12	42	15	82
Direct Costs							
Compensation							
Base Salary	$ 89,543	$ 185,000	$ 120,000	$ 162,000	$ 378,000	$ 120,750	$ 1,055,293
Benefits	$ 1,355	$ 7,500	$ 9,000	$ 18,000	$ 63,000	$ 22,500	$ 121,355
Overtime	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Bonus	$ 8,086	$ 37,000	$ 24,000	$ 32,400	$ 75,600	$ 24,150	$ 201,236
Contingent Salaries	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Other Non-Compensation							
Communications & Technology	$ 2,709	$ 15,000	$ 18,000	$ 36,000	$ 126,000	$ 45,000	$ 242,709
Occupancy	$ 6,321	$ 35,000	$ 42,000	$ 84,000	$ 294,000	$ 105,000	$ 566,321
Other (please describe)	$ 3,612	$ 20,000	$ 24,000	$ 48,000	$ 168,000	$ 60,000	$ 323,612
Total Direct Costs	$ 111,626	$ 299,500	$ 237,000	$ 380,400	$ 1,104,600	$ 377,400	$ 2,398,900
Management Fee (as necessary)	$ 14,112	$ 83,860	$ 66,360	$ 106,512	$ 309,288	$ 105,672	$ 685,804
Pass-through One-Time Costs (please describe) [1]						$ 10,000	
Pass-through Recurring Costs (please describe) [2]							$ -
Total Billing Amount	**$ 125,738**	**$ 383,360**	**$ 303,360**	**$ 486,912**	**$ 1,413,888**	**$ 493,072**	**$ 3,206,330**

Note:
All costs are per annum
[1] Pass through one time cost is 10,000 USD as a setup of the dedicated infrastructure for the Merrill Lynch teams
[2] We would suggest Copal leverages from Merrill Lynch's existing market data service contracts, and therefore would not expect a pass through cost

Work Process

A. Work Process Methodology Document

A work process methodology document will be developed to provide high quality, on-time performance at all locations (including the backup location(s)). All processes will be subject to modification as necessary to meet changing needs of Merrill Lynch. Processes may be modified only with the prior written approval of Merrill Lynch, which shall not be unreasonably withheld.

B. Documentation of Work Processes

As with all client engagements, Copal will provide detailed documentation on all aspects of the dedicated team. This will include documentation for areas such as output methodology documents (e.g., comps, profiles, risk report cards) QC process, internal project management documentation, design/format templates, workflow initiation process, escalation process, and detailed operational reporting.

C. Documentation of Staff & Management of Load Balancing

Copal Partners will document by location the staff and effectively manage the load balancing of work requests and efficiency of operations.

D. Client Communication

Merrill Lynch will have 24x7 access to an English speaking, NY-based engagement manager with strong knowledge in both investment banking, and outsourcing processes and best practices. In addition, the entire staff in India is fluent in both spoken and written English and can interface effectively with Merrill Lynch bankers at any time.

E. Work Process Guarantee

Copal Partners prides itself on standardization of process and methodology documents. A flawless work process will be developed for Merrill Lynch in order to ensure timely job completion of the highest quality. Within each layer of the process will be a system of checks of balances as well as redundancy.

Section 4.0 Proposal Form

Section 4.1 Terms of Offer

Copal Partners fully agrees to the terms (listed below) by Merrill Lynch.

Terms:

Pilot for Services: These services will be required for a 3 -4 month period. Merrill Lynch shall have the ability to cancel without penalty these services at any point during the pilot or after its completion.

Rollout of Services: The contract would be for a term of one (1) year at a time. Merrill Lynch may, at any time during the term of the contract for reasons of performance breach, terminate the contract without penalty upon sixty (60) days

written notice to Copal Partners. Additional termination provision will be contained in the agreement.

Service Fee Schedule: Copal Partners agrees to offer the services performed to Merrill Lynch at the pricing set forth in the excel spreadsheet Analytic Resources for this RFP and agrees to maintain such prices for the initial twelve (12) month term of any agreement, thereafter pricing will be reviewed annually and if applicable modified by mutual agreement of the parties.

Section 4.2 Service Fee Schedule

The excel spreadsheet indicated in section 3.1 Pricing, reflected a cost plus model which includes an itemized summary for each position required to complete the specified SOW and includes direct costs, management fees, and other pass-through costs separate by the location of the staff.

Section 5.0 Business Continuity Plans

The full Copal Partners Business Continuity Plan can be found in Appendix D.

Contingency Plan

Copal has two operating facilities in Northern India and each facility serves as a warm-standby DR site for the other. All company data is mirrored in real time between the facilities, and is also stored on tape in a secured third-party facility.

In the event of a partial or total system outage in any one of the facilities, appropriate personnel are alerted via a call tree, and sent to the backup site. Each site contains sufficient workspace and PCs to support operations at a minimum of 20% capacity. The PCs are preconfigured and on-line, and teams could be operational within 4 hours of failure. Each DR area has the same security and compliance controls (access controlled rooms, shredders, VLANS, etc) and the same support equipment (data sources, scanners, printers).

Contingency plans are reviewed and tested every six months. Additionally, we expect a dedicated DR operating facility to be operational by Q4 2006.

Security

Copal manages security according to a BS7799-certified information security management system (ISMS).

Network security controls include Cisco ASA firewalls, HP filtering routers, antivirus gateways and multiple dedicated VLANs for partitioning sensitive data to access-controlled segments of the network. Each dedicated VLAN has its own domain, file, and antivirus servers. Network and server engineers are on-site 24x7. Employees are electronically prohibited from accessing Webmail sites or from sending mail to any address outside the organization, except where required for business purposes.

Our network is secured from intrusion via redundant Cisco ASA firewalls, and further secured by HP Procurve filtering L3 switches. Dedicated client systems and servers

are segregated into protected VLANS and communication across these VLANS is electronically prohibited.

To ensure physical security, Copal's sites are manned by security guards 24x7. Access to any area within the facility requires an electronic access card when entering or leaving. Client teams work in dedicated, access-controlled rooms. Access to the delivery areas requires two separate levels of card access. Each room has its own printing, scanning, and shredding facilities, and clean desk and shredding policies are strictly enforced.

Regulatory compliance includes a trade authorization system to protect against insider trading. All employees must request authorization before making a trade on any foreign or domestic security. All employees are required to report all trading accounts, and submit statements of trades and holdings on a quarterly basis to reconcile trades and authorizations.

To ensure compliance, access, server, and network logs are all reviewed daily for unusual events. Evidences of process adherence are collected and reviewed weekly, and a complete internal ISMS audit is performed twice yearly.

Copal Partners shall exercise all reasonable care and use all reasonable procedures and precautions necessary to safeguard Merrill Lynch information and materials while within Vendor's control in order to protect same from theft, destruction, damage, misappropriation by third parties or other loss.

APPENDIX

APPENDIX A:
Responsibility Authority Statement

Proposer would agree to hold all information received from Merrill Lynch, confidential to Merrill Lynch, and shall not use, nor disclose, such information to anyone, for any purpose whatsoever, and should Proposer desire to use or release any information concerning Merrill Lynch, it shall require permission to do so, in writing, for Merrill Lynch's evaluation, by individual request and subsequent written approval or disapproval. Proposer would agree to warrant that any information generated by this RFP is considered proprietary to Merrill Lynch and shall agree not to disclose the contents, or operations, or any such information, to any source whatsoever, without the approval of Merrill Lynch. Proposer would agree not to use the Merrill Lynch name in any publication, advertisement or other public material related to this RFP, without the prior written consent of Merrill Lynch.

In the event that Proposer elects not to submit a proposal in response to this RFP, or if Merrill Lynch, upon receipt and evaluation of Proposer's bid, elects not to award a contract to Proposer for the products and/or Services described herein, Proposer agrees to return to Merrill Lynch all materials submitted by Merrill Lynch to Proposer pursuant to this RFP.

Proposer understands that Merrill Lynch reserves the right to reject any or all proposals, and to waive irregularity in this process. Failure to complete all items of this form may be cause for rejection of the proposal.

The individual submitting this Proposal represents and certifies as part of its Proposal that he/she is the person in the individual's organization authorized to act as agent for the corporation responsible for this Proposal. The costs in this Proposal have been arrived at independently, without consultation, communication, or agreement for the purpose of restricting competition, to any matter relating to costs with any other competitor or any representative of such competitor. Furthermore, Proposer agrees to the terms regarding Confidentiality and Confidential Information cited in this Request for Proposal.

Company Copal Partners Limited **Signature:** 

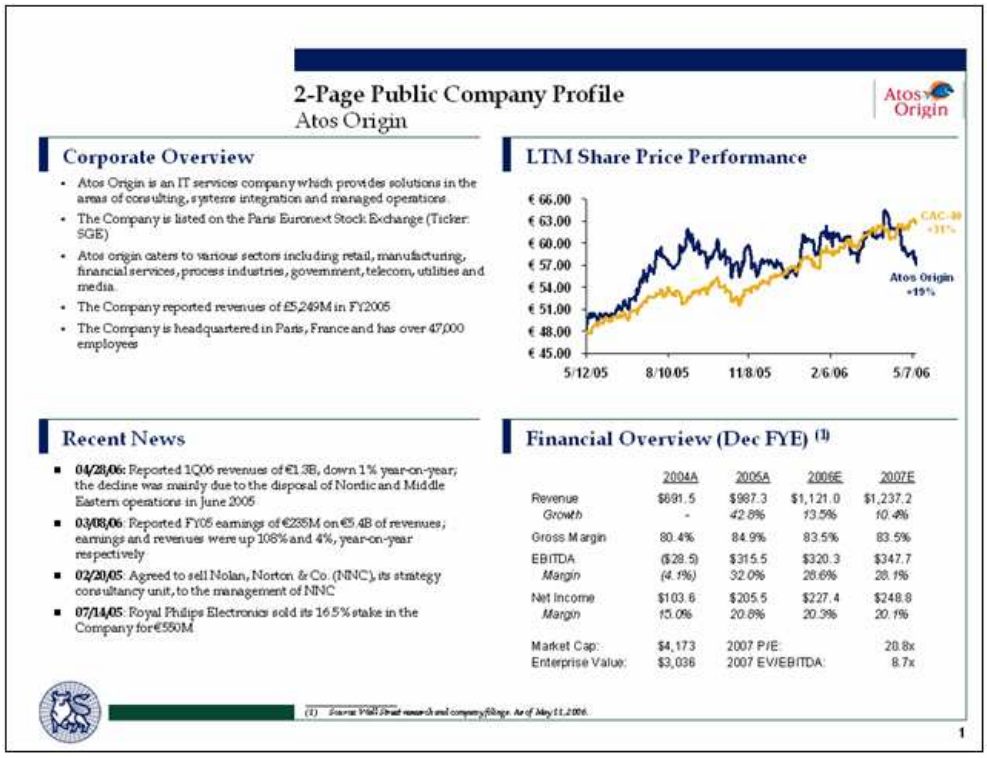
Date June 12, 2006 **Name/Title** Rishi Khosla, CEO

APPENDIX B:
Contact Persons Sheet

The Proposer is to provide information regarding individuals within the organization responsible for the contents of the response. If more than one person is identified, Merrill Lynch will assume that contacting any one of these individuals will be sufficient for correspondence relating to this RFP. Please enter this information below:

Name	Title	Telephone #	E-Mail Address
Rishi Khosla	CEO	646-662-4260	rishi_khosla@copalpartners.com
Anmol Bhandari	VP Business Development	646-361-9599	anmol_bhandari@copalpartners.com

APPENDIX C:
Merrill Lynch Sample Product Outputs



2-Page Public Company Profile
Atos Origin

Corporate Overview

- Atos Origin is an IT services company which provides solutions in the areas of consulting, systems integration and managed operations.
- The Company is listed on the Paris Euronext Stock Exchange (Ticker: SGE)
- Atos origin caters to various sectors including retail, manufacturing, financial services, process industries, government, telecom, utilities and media.
- The Company reported revenues of €5,249M in FY2005
- The Company is headquartered in Paris, France and has over 47,000 employees

LTM Share Price Performance

Recent News

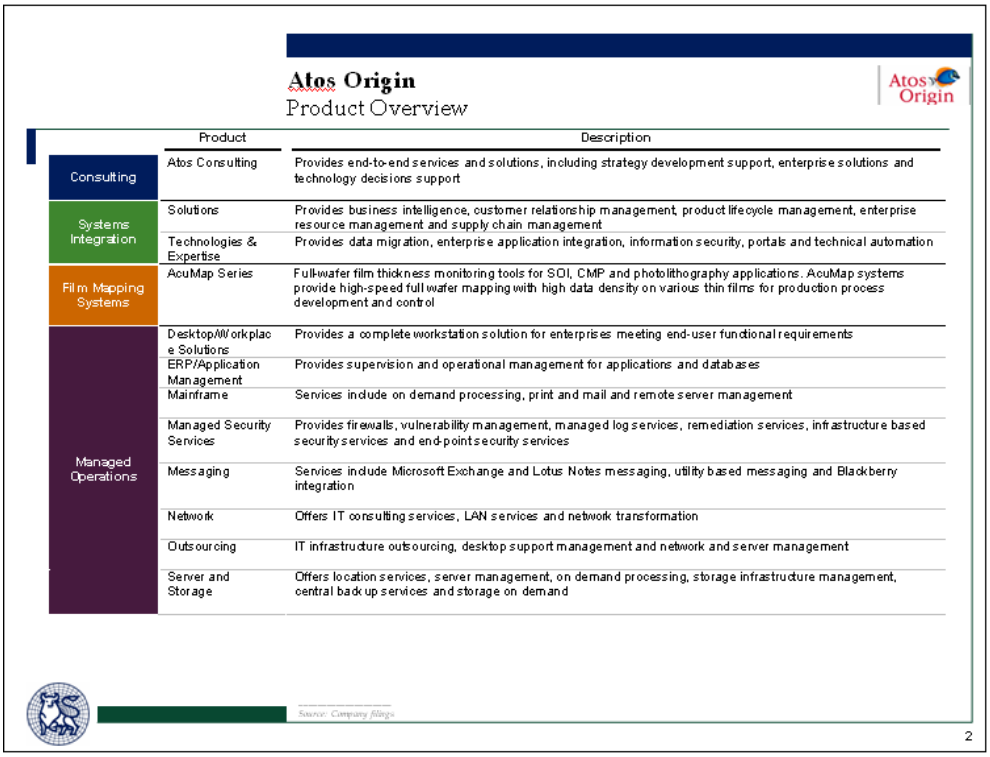
- **04/28/06**: Reported 1Q06 revenues of €1.3B, down 1% year-on-year; the decline was mainly due to the disposal of Nordic and Middle Eastern operations in June 2005
- **03/08/06**: Reported FY05 earnings of €235M on €5.4B of revenues; earnings and revenues were up 108% and 4%, year-on-year respectively
- **02/20/05**: Agreed to sell Nolan, Norton & Co. (NNC), its strategy consultancy unit, to the management of NNC
- **07/14/05**: Royal Philips Electronics sold its 16.5% stake in the Company for €550M

Financial Overview (Dec FYE) (1)

	2004A	2005A	2006E	2007E
Revenue	$691.5	$987.3	$1,121.0	$1,237.2
Growth	-	*42.8%*	*13.5%*	*10.4%*
Gross Margin	80.4%	84.9%	83.5%	83.5%
EBITDA	($28.5)	$315.5	$320.3	$347.7
Margin	*(4.1%)*	*32.0%*	*28.6%*	*28.1%*
Net Income	$103.6	$205.5	$227.4	$248.8
Margin	*15.0%*	*20.8%*	*20.3%*	*20.1%*
Market Cap:	$4,173	2007 P/E:		28.8x
Enterprise Value:	$3,036	2007 EV/EBITDA:		8.7x

(1) Source: Wall Street research and company filings. As of May 11, 2006.

1



Atos Origin
Product Overview

	Product	Description
Consulting	Atos Consulting	Provides end-to-end services and solutions, including strategy development support, enterprise solutions and technology decisions support
Systems Integration	Solutions	Provides business intelligence, customer relationship management, product lifecycle management, enterprise resource management and supply chain management
	Technologies & Expertise	Provides data migration, enterprise application integration, information security, portals and technical automation
Film Mapping Systems	AcuMap Series	Full-wafer film thickness monitoring tools for SOI, CMP and photolithography applications. AcuMap systems provide high-speed full wafer mapping with high data density on various thin films for production process development and control
Managed Operations	Desktop/Workplace Solutions	Provides a complete workstation solution for enterprises meeting end-user functional requirements
	ERP/Application Management	Provides supervision and operational management for applications and databases
	Mainframe	Services include on demand processing, print and mail and remote server management
	Managed Security Services	Provides firewalls, vulnerability management, managed log services, remediation services, infrastructure based security services and end-point security services
	Messaging	Services include Microsoft Exchange and Lotus Notes messaging, utility based messaging and Blackberry integration
	Network	Offers IT consulting services, LAN services and network transformation
	Outsourcing	IT infrastructure outsourcing, desktop support management and network and server management
	Server and Storage	Offers location services, server management, on demand processing, storage infrastructure management, central back up services and storage on demand

Source: Company filings

2

Standard Public Comparables Analysis Pages

(Dollars in Millions, Except Per Share Data)

Company	Stock Price 4/20/06	Market Cap. ($MM) (1)	Enterprise Val. ($MM) (2)	EV / Revenues 2006E	EV / Revenues 2007E	EV / EBITDA 2006E	EV / EBITDA 2007E	P/E 2006E	P/E 2007E	P/EG 2006E	P/EG 2007E
IT Services											
IBM Corp	$82.02	$127,415	$137,360	1.5x	1.4x	7.4x	6.9x	14.1x	12.8x	1.3x	1.2x
Accenture Ltd	30.16	27,201	25,494	1.5x	1.4x	9.7x	8.8x	20.9x	17.6x	1.5x	1.2x
Tata Consultancy Services Ltd	44.09	21,571	21,426	6.5x	5.3x	22.5x	19.0x	27.2x	22.7x	1.0x	0.8x
Affiliated Computer Services Inc	58.13	7,057	8,347	1.5x	1.4x	7.8x	7.2x	17.0x	15.2x	1.2x	1.1x
Capita Group plc	8.32	5,467	6,028	2.0x	1.8x	13.3x	11.7x	22.7x	19.3x	1.4x	1.2x
			Mean	2.6x	2.3x	12.2x	10.7x	20.4x	17.5x	1.3x	1.1x
Internet											
Freenet.De AG	$24.92	$1,486	$1,268	1.3x	1.1x	8.7x	7.7x	21.5x	18.1x	1.3x	1.1x
Adlink Internet Media AG	17.77	479	467	2.0x	1.5x	15.3x	10.0x	40.1x	20.6x	NA	NA
Beate Uhse AG	7.61	358	446	1.2x	NA	9.7x	NA	18.2x	NA	NA	NA
Ad Pepper Media NV	14.42	173	145	2.8x	2.2x	27.1x	16.6x	32.5x	22.5x	NA	NA
OnVista AG	17.10	115	67	4.2x	3.1x	29.1x	19.7x	63.1x	47.9x	NA	NA
			Mean	2.5x	2.0x	18.0x	13.5x	35.1x	27.8x	1.3x	1.1x
			Overall Mean	2.4x	2.1x	15.1x	11.9x	27.7x	21.9x	1.3x	1.1x

Source: Company data, Bloomberg.
(1) Market Value based on diluted shares outstanding.
(2) Enterprise Value = Market Value + Total Debt + Preferred Stock + Minority Interest - Cash & Equivalents - Short-Term Investments - Long-Term Investments.

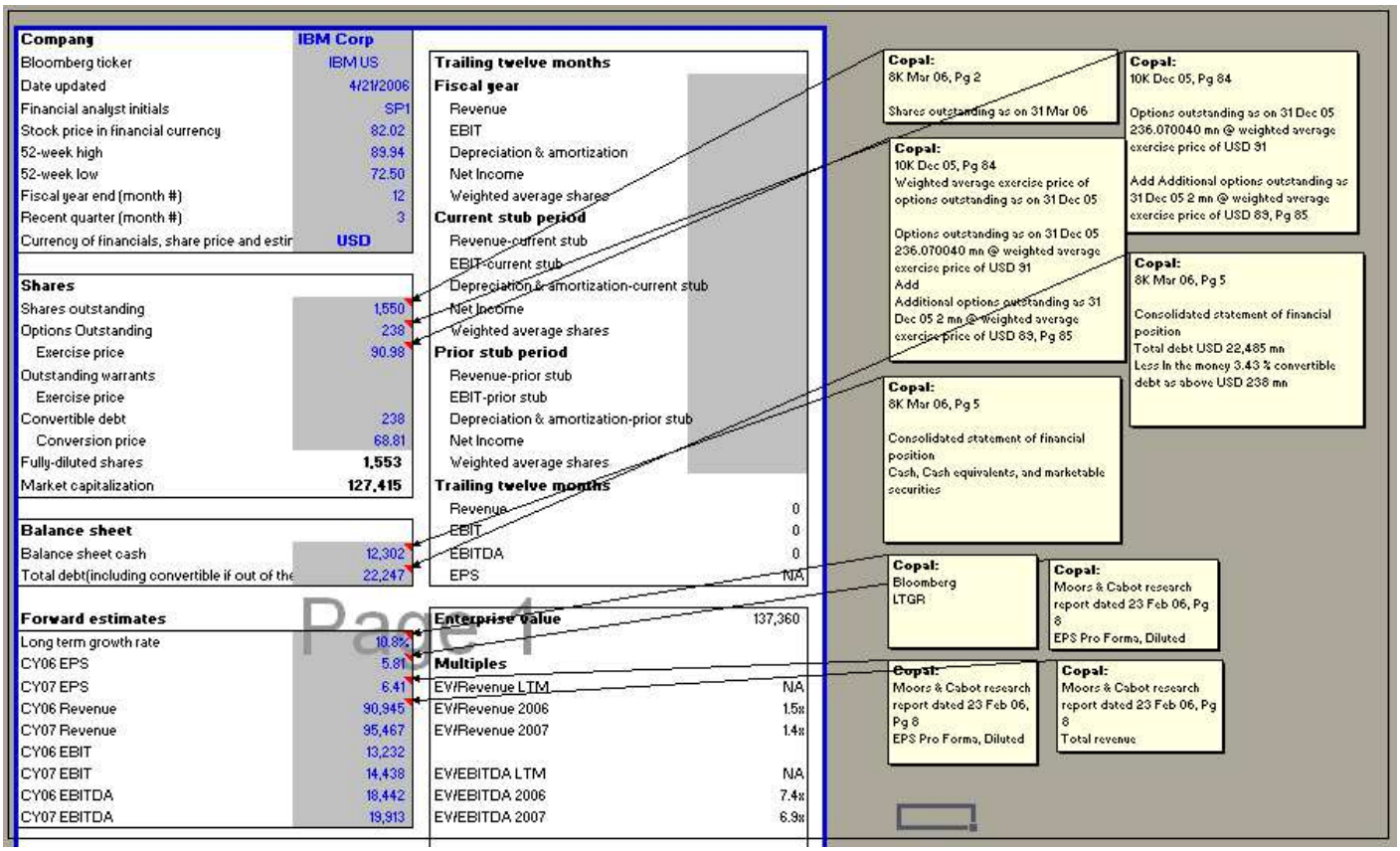
20

Acquisition Comparables Analysis Pages

Award	Target	Acquiror	Offer Value	Trans. Value	EV/Revenue LTM	EV/Revenue NTM	EV/EBITDA LTM	EV/EBITDA NTM	P/E LTM	P/E NTM
8/9/05	Technitrol Inc	LK Products Oy	$67.0	$67.0	0.98x	0.85x	7.6x	6.1x	18.8x	14.2x
5/17/05	TCL Communications	TCL & Alcatel Mobile Phones Ltd.	140.8	140.8	0.03	0.03	NA	NA	NA	NA
11/17/04	CTS Corporation	SMTEK International Inc	44.6	59.1	0.58	0.55	10.1	9.2	19.8	8.3
6/14/04	UTStarcom Inc	Wireless Handset business of Audiovox	165.1	165.1	0.18	0.15	NA	NA	56.5	NA
2/27/04	Ahlstrom Capital Oy	Industrial Elec. business of Elcoteq	40.0	40.0	0.32	0.30	2.9	2.1	NA	NA
		Max			0.98x	0.85x	10.1x	9.2x	56.5x	14.2x
		Mean			0.42	0.37	6.9	5.8	31.7	11.2
		Median			0.32	0.30	7.6	6.1	19.8	11.2
		Min			0.03	0.03	2.9	2.1	18.8	8.3

Source: Press Release, Filings, and Bloomberg

Merrill Lynch Sample Product Outputs (cont.)



APPENDIX D:

Information Security Questionnaire

Version 9.1

Company Name: Copal Partners

Name of person who completed this form: Bijit Borah

Title of person who completed this form: Head of Technical Operations

Telephone number of person who completed this form: +91 9350559120

Email address: bijit_borah@copalpartners.com

Date Completed: 06/12/06

TABLE OF CONTENTS 2

Introduction

The Information Security Questionnaire is provided by the Merrill Lynch department of Information Security & Privacy (IS&P). Your responses to the questionnaire will be reviewed by Merrill Lynch IS&P to ensure compliance with legislative, regulatory and industry standards governing, among other things, the confidentiality, integrity, and privacy of Merrill Lynch data.

Completing the Questionnaire

We ask that you answer all questions. Most questions can be answered with a YES, NO, or NA (Not Applicable) response. If you answer NO or NA, please provide a written explanation in the space provided. If work is planned or in progress to meet a requirement not currently met, a NO answer should be followed with a timeframe in which the requirement will be met. Questions that are not applicable to the services anticipated by an agreement can be answered with an NA response.

Some questions list multiple choice answers. Please check those that apply and provide an explanation for those you do not check.

Additional Information

In some instances the questionnaire will not provide enough information for Merrill Lynch IS&P to perform a complete assessment. In those instances Merrill Lynch IS&P may need to engage the Vendor in further discussions or perform an on-site assessment.

General Requirements

Vendor confirms that it will:

Employ staff whose primary responsibilities include information security and information risk management.

☒ Yes ☐ No

Explanation:

Name and title of the officer who has this responsibility: Vijay Tangri, Head of Compliance

Establish and implement information security policies, processes and procedures that govern:

☒ Appropriate staff use of the Internet, electronic mail, voice mail and facsimile machines

☒ Vendor staff remote access to Vendor-owned and operated networks and systems, with user-level privileges

☒ Vendor staff remote access to Vendor-owned and operated networks and systems, with administrator-level privileges

☒ Personnel management (including procedures to be followed when a staff member leaves Vendor's employ)

☒ Backup, recovery, and archival of Vendor-owned information

☒ Backup, recovery, and archival of Customer-owned information

☒ Secure operating system and software application configuration and management

☒ Access to, processing of and disposal of customer-owned information

☒ Computer security incident response and investigation

☒ Security vulnerability notification and remediation

☒ Protection against malicious code and viruses

☒ Business continuity and disaster recovery

☒ Change management

☒ Physical security

Establish and implement a training and awareness program to communicate to all staff the policies, processes, and procedures defined in section J of this questionnaire.

☒ Yes ☐ No

Explanation: All employees are given compliance and security training on induction, and refresher trainings are given quarterly.

Agree to follow a documented management approval process to handle exceptions to the policies and processes defined in Section J.

☒ Yes ☐ No

Explanation:

Agree to provide copies of relevant policy, process, and procedure documents to Merrill Lynch.

☒ Yes ☐ No

Explanation:

Agree to adhere to a software design, development, testing, and deployment "life cycle" methodology for all software releases, and to integrate information security and information risk management into all phases of the methodology.

☐ Yes ☐ No ☒ NA

Explanation:

Should Vendor receive Merrill Lynch approval for a third party to provide all or part of the services anticipated by an agreement with Merrill Lynch, Vendor has appropriate programs in place for third party oversight and due diligence.

☒ Yes ☐ No ☐ NA

Explanation:

Agree not to post any information or inquiry to any public forum including, but not limited to Internet Newsgroups, for which said information can be traced or related to Merrill Lynch.

☒ Yes ☐ No

Explanation:

Monitor, on a regular basis, reputable sources of computer security vulnerability information such as FIRST, CERT/CC, BugTraq and other Vendor mailing lists, and take appropriate measures to obtain, thoroughly test, and apply relevant service packs, patches, upgrades and workarounds. Critical fixes should be tested and implemented in an expedited manner. Those of potentially lesser impact should be implemented within a reasonable time.

☒ Yes ☐ No

Explanation:

Test, on at least a quarterly basis, the implementation of its information security measures through the use of network, system, and application vulnerability scanning tools and/or penetration testing. Provide test results pertaining to services anticipated by an agreement with Merrill Lynch, and a plan for resolving any problems, to Merrill Lynch within ten (10) business days of the completion of the test.

☒ Yes ☐ No

Explanation:

Contract, on at least an annual basis, with a reputable information security consulting firm to perform a comprehensive security assessment, including review of policies, processes and procedures, as well as on-site assessment of physical security arrangements and penetration testing. Provide assessment results pertaining to services anticipated by an agreement with Merrill Lynch, and a plan for resolving any problems, to Merrill Lynch within ten (10) business days of the completion of the assessment.

☒ Yes ☐ No

Explanation: Ernst & Young are our external consultants for BS7799 implementation.

Permit Merrill Lynch to request and/or perform, at the expense of Merrill Lynch, up to two additional security assessments per year, including but not limited to, review of policies, processes, and procedures, on-site assessment of physical security arrangements, network, system, and application vulnerability scanning, and penetration testing. Such assessments will be conducted at a time mutually agreed upon between Vendor and Merrill Lynch, and the results will be provided to Vendor by Merrill Lynch.

☒ Yes ☐ No

Explanation:

Permit Merrill Lynch to conduct security vulnerability (penetration) testing on the Hosting Environment upon 48 hours prior notice to Vendor. Vendor hereby authorizes such security testing and agrees to cooperate with Merrill Lynch in their implementation. Merrill Lynch may elect to retain a third party firm to conduct such security testing. Security testing may include security penetration tests by electronic methods (for example, "Black Box" penetration tests over the Internet).

☒ Yes ☐ No

Explanation:

Permit Merrill Lynch to conduct code reviews ("Gray Box" tests) on the Applications used in the performance of the services under the terms of the contract. Merrill Lynch may elect to retain a third party firm to conduct such Gray Box tests and will do so under the mutual agreed upon terms with the Vendor.

☒ Yes ☐ No

Explanation:

Upon conclusion or termination of the services anticipated by an agreement, provide Merrill Lynch with copies of all Merrill Lynch information, as well as all backup and archival media containing Merrill Lynch information.

☒ Yes ☐ No

Explanation:

Upon conclusion or termination of the services anticipated by an agreement, use mutually agreed upon data destruction processes (as approved and certified by each Vendor and Merrill Lynch Information Security) to eliminate all Merrill Lynch information from Vendor systems and applications.

☒ Yes ☐ No

Explanation:

At the time of initial user sign-on to any system, device, and/or application used to provide services anticipated by an agreement, the system, device, and/or application must display a message advising users that the system they are accessing is for authorized use only and activities are monitored and recorded. The message should also include content that advises prospective users that unauthorized and/or malicious use of the system is prohibited and violators may be prosecuted to the fullest extent of the local and international law and that by logging on, the user has read and understood these terms. The following is solely for example purposes:

********** *WARNING* **********

You have accessed a private computer system. This system is for authorized use only and user activities are monitored and recorded by company personnel. Unauthorized access to or use of this system is strictly prohibited and constitutes a violation of federal and state criminal and civil laws, including Title 18, Section 1030 of the United States Code and applicable international laws. Violators will be prosecuted to the fullest extent of the law. By logging on you certify that you have read and understood these terms and that you are authorized to access and use this system.

☒ Yes ☐ No

Explanation:

Network & Communications Security

Vendor confirms that it will:

At the hosting facility, deploy multiple layers of defense (e.g. firewalls, network intrusion detection, and host-based intrusion detection) to increase the effort required to compromise network(s), system(s) or application(s) and to increase the probability that such attempts will be detected *(check all that apply)*.

☒ NIDS
☒ HIDS
☒ Firewalls
☒ Proxy Services
☒ NAT

➔ If any of the above are NOT checked, please explain:

Deploy firewalls, filtering routers, or other similar network segmentation devices between Production networks providing services anticipated by an agreement and Vendor's corporate networks to minimize the potential for unauthorized access.

☒ Yes ☐ No

Explanation of what you currently have deployed: We have redundant Procurve filtering routers deployed between different production VLANS and our corporate VLANS.

All security monitoring systems including, but not limited to, firewalls and intrusion detection systems must be monitored 24 hours per day, 365 days per year.

☒ Yes ☐ No

Explanation:

Obtain written approval from Merrill Lynch before making any change to firewall or router configurations that would affect access to the networks and systems used to provide services anticipated by an agreement.

☒ Yes ☐ No

Explanation:

Configure its firewalls, network routers, switches, load balancers, name servers, mail servers, and other network components in accordance with the recommendations of applicable Internet Engineering Task Force Request for Comments documents (e.g., RFC2182 - Selection and Operation of Secondary DNS Servers, RFC2505 - Anti-Spam Recommendations for SMTP, RFC2644 - Changing the Default for Directed Broadcasts in Routers, and RFC2827- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing).

☒ Yes ☐ No

Explanation:

Infrastructure Platforms, Services & Operations Security

Vendor confirms that it will:

Configure all infrastructure platforms and services (operating systems, web servers, database servers, firewalls, routers, etc.) used to provide services anticipated by an agreement according to industry best practices.

☒ Yes ☐ No

Explanation:

Restrict user accounts on each system used to provide services anticipated by an agreement to those Vendor staff members with a job-related need to access the system.

☒ Yes ☐ No

Explanation:

Use commercially reasonable efforts to ensure that the authentication mechanisms used to control access to each system used to provide services anticipated by an agreement are configured to prevent the use of trivial and predictable authenticators. Strong authentication, such as token-based authentication, should be applied to users with access to critical business applications or systems, special access privileges, administrative privileges, or remote access to systems and/or network devices. If passwords are used as a part of the authentication process, they must adhere to the following Merrill Lynch specified characteristics for minimum length and character set mix:

Passwords must be at least six characters long
Characters must come from at least three of the following categories:
Upper case letters (A, B, C, ... Z)
Lower case letters (a, b, c, ... z)
Numbers (0, 1, 2, ... 9)
Non alphanumeric

☒ Yes ☐ No

Explanation:

Maintain logically separate development, quality assurance, test, and production operating environments as it relates to services anticipated by an agreement.

☒ Yes ☐ No ☐ NA

Explanation:

Ensure that developers do not have access to Merrill Lynch or Vendor production systems or production data. If access to production systems is required, Vendor agrees to access systems in accordance with a documented Controlled Access to Production (CAP) policy.

☐ Yes ☐ No ☒ NA

Explanation: ML-related services do not require any custom applications, so no developers will be provided access to production systems or data.

Ensure that all remote administrative access to production systems is performed over encrypted connections (i.e., SSH, SCP, SSL-enabled web-management interfaces, and VPN solutions). Access will be limited to authorized personnel and logged (e.g., employee ID, time stamp, etc.). Logs will be reviewed on a regular basis.

☒ Yes ☐ No\

Explanation:

Ensure that time-of-day clocks on all systems and network devices are synchronized to permit audit reconciliation of transactions (any type) between systems.

☒ Yes ☐ No

Explanation:

Unless required otherwise by law, at a minimum, logs must be maintained for a period of no less than thirty (30) days online and seven (7) years offline from origination and should include the following data as applicable and/or available by the system or device *(check all that apply):*

☒ All sessions established

☒ Information related to the reception of specific information from a user or another system

☒ Record the link received information with the originator of the information

☒ Failed user authentication attempts

☒ Unauthorized attempts to access resources (software, data, processes, etc.)

☒ Administrator actions

☒ Administrator disabling of audit logging

☒ Events generated (e.g., commands issued) to make changes in users' security profiles and attributes

☒ Events generated to make changes in the security profiles and attributes of system or application interfaces

☒ Events generated to make changes in permission levels needed to access a resource

☒ Events generated that make changes to the system or application security configuration

☒ Events generated that make modifications to the system or application software

☒ Events generated that make changes to system resources deemed critical (as determined by the administrator)

➔ If any of the above are NOT checked, please explain:

Collected logging must provide sufficient information that would permit a forensic capability to recreate the event.

☒ Yes ☐ No

Explanation:

All Log files should be protected against unauthorized access, modification, or deletion and be able to satisfy an evidence requirement for chain of custody.

☒ Yes ☐ No

Explanation:

At the request of Merrill Lynch, provide copies of any log file maintained by Vendor (including firewall, intrusion detection, system, and application log files) to support any investigation or legal action that may be initiated by Merrill Lynch.

☒ Yes ☐ No

Explanation:

Application Security

Vendor confirms that the application(s) anticipated by an agreement with Merrill Lynch will:

Permit only authenticated and authorized users to view, create, modify, or delete information managed by the application. Such authentication and authorization shall be provided through the use of individual, per-user user-id and password unless otherwise specified by Merrill Lynch.

☒ Yes ☐ No

Explanation:

Ensure that the authentication mechanism used to control access to the application is configured to prevent the use of trivial and predictable authenticators. Strong authentication, such as token-based authentication, should be applied to users with access to critical business applications, sensitive information, special access privileges, or with external access capabilities. If passwords are used as a part of the authentication process, they must adhere to Merrill Lynch specified characteristics for minimum length and character set mix defined at Section C, Question 3.

☒ Yes ☐ No

Explanation:

Require each user of the application to be uniquely and unambiguously identified through the use of an identifier such as a user-id.

☒ Yes ☐ No

Explanation:

Ensure that web browser cookies that store/contain confidential data will be encrypted using a public and widely accepted encryption algorithm. This encryption will be performed independently of any transport encryption such as Secure Sockets Layer.

☐ Yes ☐ No ☒ NA

Explanation: Our services only require Windows 2003 file services, and do not require confidential information to pass through the web browser.

"Time out" and terminate the user session after a mutually agreed upon period of user inactivity. After this timeout, the user must re-authenticate to the application before any further work may be performed.

☒ Yes ☐ No

Explanation:

Terminate any active sessions interrupted by power failure, system "crash," network problem, or other anomaly, or when the connection is interrupted by the user.

☒ Yes ☐ No

Explanation:

The audit log, at the application level, should record, at a minimum *(check all that apply)*:

☒ Date and time of the attempted event
☒ User-id of the initiator of the attempted event
☒ Names of resources accessed
☒ Host name the user connected from
☒ Success or failure of the attempt
☒ Event type

➔ If any of the above are NOT checked, please explain:

Data Security

Merrill Lynch will identify to Vendor the classification level(s) that should be assigned to all Merrill Lynch information anticipated by an agreement with Merrill Lynch.

Vendor confirms that it will:

Transmit all Merrill Lynch confidential information using Secure Sockets Layer (SSL) or Transport Layer Security protocol and no less than 128-bit keys. For non web-based applications or services, transmit all Merrill Lynch confidential information via a secure mechanism other than a Web browser.

Vendor will provide Merrill Lynch IS&P a detailed design document which describes the cryptosystem including the:

Algorithm choices
Key length
Key Management
Key Exchange
Pseudo random number generation

Merrill Lynch IS&P will review and provide a direction based on the Vendor's criteria.

☒ Yes ☐ No

Explanation: Secure transmission can be arranged via ssl websites, sftp, or ipsec vpn as per Merrill Lynch's requirements.

When database storage is required, store all "Confidential" Merrill Lynch information in a database that is *(check all that apply)*:

☒ Logically separate
☐ Physically separate

Explanation: No databases will be used for service. If a database is required, a physically or logically separate database can be arranged as per Merrill's requirements.

Limit access to all Merrill Lynch information anticipated by an agreement with Merrill Lynch to those Vendor staff with a need-to-know, and require all such staff members to sign a confidentiality agreement;

☒ Yes ☐ No

Explanation:

Maintain separate and distinct development, test and staging, and production databases to ensure that production information is not accidentally altered or destroyed.

☒ Yes ☐ No ☐ NA

Explanation:

Testing should be done only with test data that is free of Merrill Lynch confidential information. Production data cannot be used in testing, quality assurance, or development environments.

☒ Yes ☐ No ☐ NA

Explanation:

Vendor will ensure that in the event of a computer hard drive failure, the hard drive will not leave the Vendor facility for repairs without first ensuring that the data is no longer required. It should be scrubbed clean of all data through the use of a commercial software product that ensures a minimum of 4 passes across the media or through the use of a degaussing device. If the data is required, Vendor will notify Merrill Lynch to identify what course of actions are required to recover the data for further processing.

☒Yes ☐ No

Explanation: No working hard drive would leave a dedicated client room and / or the facility without first being scrubbed by disc wiping software. Any hard drive that crashes is put into a locked room.

Dispose of confidential information as follows *(check all that apply)*:

☒ Paper – Confidential information contained on hard copy will be disposed of by shredding.

☒ Non-Paper Storage Media (e.g. tapes, computer discs, microfilm and microfiche) – Describe your process for destruction: These items are shredded in an industrial shredder.

☒ Computer Hardware – Extreme caution will be taken when disposing of PC's, laptops or other devices used to store confidential information. These devices must be cleared of all confidential information before they are destroyed, sent to a Vendor to be refurbished, donated to charity, or transferred in any way. Describe your process for destruction: Explanation: No working hard drive would leave a dedicated client room and / or the facility without first being scrubbed by disc wiping software. Any hard drive that crashes is put into a locked room

☒ A disk wipe utility or physical device must be used to fully erase all Vendors and all Merrill Lynch prior to disposal or transfer of any equipment containing a hard drive, removable media, or any media with data storage capabilities. Describe your process for destruction: Explanation: No working hard drive would leave a dedicated client room and / or the facility without first being scrubbed by disc wiping software. Any hard drive that crashes is put into a locked room

☒ Leased systems must be completely cleared of Vendor and all Merrill Lynch information (data records) before being returned to the leasing company. Describe your process for destruction: Explanation: No working hard drive would leave a dedicated client room and / or the facility without first being scrubbed by disc wiping software. Any hard drive that crashes is put into a locked room

➔ If any of the above are NOT checked, please explain:

Physical Security

Vendor confirms that it will:

Maintain all workstations, servers, and network equipment used to provide services anticipated by an agreement in secure facilities owned, operated, or contracted for by Vendor;

☒ Yes ☐ No

Explanation: This will include leased equipment as well.

Limit access to these secure facilities to authorized Vendor staff members with job-related needs;

☒ Yes ☐ No

Explanation:

Based on risk, areas in which workstations containing or access *any* Merrill Lynch information must have physical and environmental controls commensurate with potential threats.

☒ Yes ☐ No

Explanation:

Monitor access to these secure facilities through the use of security guards, surveillance cameras, authorized entry systems, or similar methods capable of recording entry and exit information;

☒ Yes ☐ No

Explanation:

A Vendor employee must escort all visitors and all visitors must be signed in throughout the time that the visitor is in a Vendor facility.

☒ Yes ☐ No

Explanation:

Maintain all backup and archival media containing Merrill Lynch information, or other information used to provide services anticipated by an agreement, in secure, environmentally-controlled storage areas owned, operated, or contracted for by Vendor;

☒ Yes ☐ No

Explanation:

Limit access to backup and archival media storage areas and contents to authorized Vendor staff members with job-related needs.

☒ Yes ☐ No

Explanation:

The statutory disqualification rules of the SEC and NYSE restrict individuals with criminal backgrounds from performing work in the securities industry.

Please describe what processes you have in place to perform criminal background checks with respect to your employees who may be performing services for Merrill Lynch under the services anticipated by an agreement with Merrill Lynch: All employees have full background checks via a verification agency. The agencies check their addresses (permanent and present) and their criminal records from their respective police stations. Employees with questionable backgrounds are not hired.

Vendor shall ensure that any computers used to manage the Merrill Lynch project requiring technical support (e.g. hard drive failure, application support) be serviced *only* by person(s) who have had a criminal background check completed in accordance with the requirement F-7.

☐ Yes ☒ No

Explanation: We require that our hardware / computer vendors and technicians screen their employees for criminal records as per best practice in India.

In all cases where a violation is discovered by Vendor personnel of any law, regulation or corporate policy, Vendor shall immediately notify Merrill Lynch, which shall have sole discretion as to whether such personnel should be given, or continue to have, access to any data, system, or project on behalf of Merrill Lynch under the services anticipated by an agreement with Merrill Lynch.

☒ Yes ☐ No

Explanation:

Vendor will provide Merrill Lynch IS&P with a statement or policy that describes their position on the use of photography within or around their facility. This includes the use of video surveillance for security purposes.

☒ Yes ☐ No

Explanation:

Maintain a documented policy and procedure for handling the removal of non-personal property removed from secured areas (e.g., a Property Removal Pass). Authorizations by Vendor management must precede any equipment, information or software being taken off-site. This process must be audited monthly by management level personnel.

☒ Yes ☐ No

Explanation:

Ensure that out-going property is recorded and that Property Removal Passes are verified and maintained.

☒ Yes ☐ No

Explanation:

Vendor must implement appropriate physical and environmental controls. Physical access controls must include those that restrict and monitor entry to the Vendor's facility (e.g. data or network operations centers, telecommunications rooms, or ancillary areas (i.e. generator or UPS storage rooms), and should be implemented as follows *(check all that apply)*:

☒ Access will be limited to a need-to-know/use basis, and will be kept to a minimum.

☒ Vendor or building custodian will review physical access privileges on a semi-annual basis

☒ Physical entry to sensitive areas (data or network operations centers, UPS areas, etc.) must be minimally controlled by electronic card access locks

☒ Closed circuit television used on all doors providing access to the facility and all sensitive areas

☒ Physical and logical access will be removed and/or disabled within 24 hours of termination of Vendor personnel.

➔ If any of the above are NOT checked, please explain:

Protection Against Malicious Code

"Malicious code" or "Malware," for the purposes of these requirements, includes any software or scripts developed to do harm to computer systems and data. Examples of malicious code include: viruses, worms, Trojan horses and spyware / adware, In addition, malicious code can take the form of ActiveX controls, Java applets, word processing macros, spreadsheet macros and web or operating system scripts. We expect Vendor to use its best efforts to defend against these threats and also to explain how it will go about this.

Vendor confirms that it will:

Use commercially available virus and malicious code detection and protection product(s) on all workstations and servers used to provide services anticipated by an agreement.

☒ Yes ☐ No

Explanation:

Maintain installed virus and malicious code detection and protection product(s) at the latest available signature levels.

☒ Yes ☐ No

Explanation:

Report all occurrences of viruses and malicious code, not handled by deployed detection and protection measures, on any workstation or server used to provide services anticipated by an agreement, to Merrill Lynch within four (4) hours of discovery. Thereafter, updates to be provided to Merrill Lynch every eight (8) hours (or at mutually agreed upon times) for the duration of the incident. This report must be made by calling 1-800-MER-HELP (637-4357). The attendant will input a trouble ticket and route it to the IS&P queue.

☒ Yes ☐ No ☐ NA

Explanation:

Computer Security Incident Response

Vendor confirms that it will:

Have a detailed, documented plan for responding to computer security incidents that includes processes and procedures for assessing the severity of the incident, identifying the cause of the incident, repairing the cause of the incident, restoring normal operations, and documenting the results of the response;

☒ Yes ☐ No

Explanation:

Report the detection of any computer security incident involving the networks, systems, or applications used to provide services anticipated by an agreement with Merrill Lynch with an IMMEDIATE call to Merrill Lynch. Thereafter, updates to be provided to Merrill Lynch every four (4) hours (or at mutually agreed upon times) for the duration of the incident. The reports should include status, direction, and disposition of the incident. This report must be made by calling 1-800-MER-HELP (637-4357). The attendant will input a trouble ticket and route it to the IS&P queue.

☒ Yes ☐ No ☐ NA

Explanation:

Follow industry best practices when collecting and preserving evidence during an incident investigation;

☒ Yes ☐ No

Explanation:

Provide Merrill Lynch, within five (5) business days of the closure of the incident, with a written report describing the incident, actions taken during the response, and plans for future actions to prevent a similar incident from occurring in the future.

☒ Yes ☐ No

Explanation:

Please describe your process to prevent or detect unauthorized access to non-Public confidential information (this includes systematic and physical intrusion perpetrated by an employee, business partner/vendor, or unknown party):

Copal has multiple layers of physical and electronic security and monitoring to prevent and detect access to confidential information. Security is managed according to our BS7799/ISO7799 Information Security Management System. Copal Partners has been certified by the British Standards Institute in this regard.

With regard to physical security, every door in the facility is controlled by electronic access control systems and monitored by CCTV and 24x7 security guards who enforce a strict no tailgating policy. Access to each work room is given on a job-requirement basis only. Work rooms have dedicated printing and shredding facilities, and whole pieces of paper are not allowed out of work rooms. Additionally, employees are required to comply with strict clean desk and clear screen policies to prevent leakage of confidential information. To detect unauthorized access, CCTV cameras are monitored 24x7 by security personnel. A second CCTV viewing terminal and a recording center is placed in a separate, access-controlled room. Access logs and CCTV data are reviewed on a daily basis.

For network security, dedicated teams work on private, segregated VLANs with their own file and domain servers, as per client requirements. Access to data areas is protected by username and password, and is granted according to least-required-privilege principles. Access and changes to this data are logged using best-practices Windows auditing, and are reviewed regularly.

Except where required for business reasons, employees are electronically prohibited from sending email to any outside domains or from viewing web-based email sites. To further prevent data leakage, CD drives, floppy

drives, and USB ports are disabled on all PCs. Personal laptops and removable media devices are prohibited in the facility.

Please describe your process to manage detection, and resolution in each of the incident types identified here:

unauthorized access to information (electronic or hard copy), including processing errors that result in the unauthorized release of personal information): Copal will not handle personal information of Merrill's employees or clients. Copal personal information hardcopies are locked in secure cabinets in a workroom which is closed by electronic access controls. Softcopies are stored on secure file systems which are audited for object access and reviewed regularly.

break-ins of your office spaces including data centers: Copal will not handle personal information of Merrill's employees or clients. Copal has 24x7 security within the office with at least 1 person at each entrance/exit at all times. Our data centers are manned by IT staff 24 hours, and have electronic access control as well as CCTV. CCTV is continuously monitored by security and logged. Access control logs are reviewed on a weekly basis.

theft of computer equipment or components: Copal will not handle personal information of Merrill's employees or clients. All equipment entering or exiting the building must be accompanied by a signed gate pass issued by management. Assets are tagged and their serial numbers are recorded. Any asset being carried in on a temporary basis has its serial number recorded and is reconciled upon exit from the building.

Has any incident resulted in notification to your client(s)?

☐ Yes ☒ No ☐ NA

Explanation: Copal has never had a known breach of security.

Has any incident resulted in the involvement of regulators or law enforcement?

☐ Yes ☒ No ☐ NA

Explanation:

Has any incident resulted in the termination of employees or vendors?

☐ Yes ☒ No ☐ NA

Explanation:

Business Continuity & Recovery

Vendor confirms that it will:

Allow Merrill Lynch to review the Vendor Business Continuity Plan if the scope of services anticipated by an agreement call for a level of Business Continuity.

☒ Yes ☐ No

Explanation:

Have a detailed, documented plan for responding to a prolonged disruption in services caused by power failure, system failure, natural disaster, or other unforeseen circumstances that includes processes and procedures for resuming operations within a mutually agreed upon time period.

☒ Yes ☐ No

Explanation:

Test, on at least an annual basis, the implementation of this plan. The results of each test, and a plan for resolving any problems discovered in a timely manner, will be documented and such documentation provided to Merrill Lynch within five business days of the completion of the test;

☒ Yes ☐ No

Explanation:

Report the activation of this plan to Merrill Lynch within one (1) hour of activation, and provide regular status updates at four-(4) hour intervals (or at mutually agreed upon times) for the duration of the recovery period.

☒ Yes ☐ No

Explanation:

Perform backups of all systems, applications, and data used to provide services anticipated by an agreement in a manner that will support the aforementioned Business Continuity Plan.

☒ Yes ☐ No

Explanation:

Periodically transfer backup media to a secure off-site storage facility.

☒ Yes ☐ No

Explanation:

Maintain a record of all backup transfers that can be audited to ensure all materials are accounted for.

☒ Yes ☐ No

Explanation:

Documentation Requirements

In order to ensure that all necessary security provisions are met, Merrill Lynch requires Vendor documentation on the following areas to be submitted along with this document for review. Alternatively, if a Site Assessment visit to Vendor facility is undertaken, these documents can be presented for Merrill Lynch review during that visit. In either case, please check the boxes below to indicate that the indicated documentation exists.

Information Security Policies & Processes:

- ☒ Software and System Change Management
- ☒ Software Physical Installation & Network Download
- ☒ Removal and Physical Transport of Data Storage Devices
- ☒ Electronic Communications (email, voicemail, Internet, instant messaging, facsimile)
- ☒ Telecommuting & Remote Access
- ☒ Data & Information Privacy
- ☒ Data Integrity
- ☒ Physical Security
- ☒ Incident Response (process/plan including all incident reporting sources)
- ☒ Virus/Malicious Code
- ☒ Vulnerability Management
- ☒ Confidential Information Storage & Destruction (all storage device types)
- ☒ Controlled Access to Production (CAP) policy used to provide developer access to production systems or information

Technical Standards & Guidelines

- ☒ Authentication
- ☒ Configuration Standards for Operating Systems
- ☐ Database Security: Copal does not have any database servers.
- ☐ Web Server Security: Copal does not have any public web servers.
- ☒ Network Security ☒☒

Business Continuity

- ☒ Disaster Recovery & Contingency Planning

Logical Data Flow Diagrams ☒

- ☐ Including corresponding Merrill Lynch data for proposed application(s):

Copal does not use any data processing applications.

Network Topology Diagram

☐ For all Merrill Lynch data and relevant data processing applications, please show the placement of data storage devices, network transport/switching elements, network monitoring devices and physical data transport paths. Typical devices might include firewalls, load balancers, packet sniffers, modems, wireless access points, network and host intrusion detection functions etc.):☒☒
Copal does not use any data processing applications.

Data Transport & Security Protocols

☐ Please provide a detailed description of how all protocols and services are used in the applications/systems described in the Network Topology diagram (e.g., HTTP, SSL, FTP, SMTP, SNMP, SunRPC, DCOM, NTLM, ODBC, SOAP, CORBA, etc.).:
Copal does not use any data processing applications.

☒☒Proprietary or Modified Protocols

☐ Please provide details about the purposes of the protocol, why a non-standard protocol is needed and the security features offered by the protocol :
Copal does not use any data processing applications or non-standard
protocols.

Independent Auditor Reporting

☒ Other independent auditors report.
☐ SAS-70 type 2 independent auditors report.

Vendor Oversight (Third Party)

☒ Vendor engagement process.
☒ Vendor oversight program.

If you are not providing all of the required documentation, it is important that you explain in the space provided:

ISMS/L2
Business Continuity Plans

APPENDIX E:

Copal Business Recovery Plan

Copal Partners

Executive Summary

The mission of the Copal Research's DR team and this document to help ensure timely recovery of critical business operations of Copal Research after a business interruption and return back to normalcy.

Based on Copal Research's preparation for handling risks that threaten the continuity of business process the strategy is to use existing infrastructure and add certain critical components, like procedures of backup tape testing for restorability, ensure SLA with vendors, identify cold standby sites for restarting equipment and/or storage of DR tapes. This would be the first level contingency plan for DRP.

The crisis management plan will be tested at regular frequencies of at least once every three months, and staff to be given adequate training and skill upgrade in the areas required.

Copal Research now needs to take the way ahead, and start putting together the components required for its business functions. As of now, the identified applications are the Windows File Services, Messaging services and Backup Services. Also, other avenues would be explored like stocking spares on site or having a SLA with the vendor, exploring insurance options, identifying cold standby site facilities.

Copal Research has the primary DR Head identified as the Mr. Bijit Borah and alternative contact as Mr. Puneet Guglani. The DR team for Copal Research would also be responsible for the Disaster Recovery Plan.

1 INTRODUCTION

There are many risks that may threaten an organization by disrupting the business processes. These risks include traditional emergencies like fires, floods, earthquakes and tornados as well as risks from physical and cyber terrorism, cyber crime, computer and telecommunications failures, theft, employee sabotage, and labor strife. Any one of these can all be very disruptive for the business.

Disaster Recovery Plan (DR) can be defined as 'the processes, procedures, decisions and activities to ensure that an organization can recover and continue to function through an operational interruption. The aim of DR is to achieve a cost-effective contingency and recovery solution that balances the value of potential losses to the business and its assets against the cost of guaranteeing continuity of critical business processes. Service levels may be reduced due to business interruption but through good planning, a minimum level of service can be provided and a perception of business as usual conveyed to the customer or client.

1.1 MISSION AND OBJECTIVES

Mission:

To ensure timely recovery of critical business operations of Copal Research after an interruption and return back to normalcy.

Objectives:

1. Develop cost effective Business resumption plan (based on the recovery strategy) to ensure smooth operation of critical functions.
2. Define Roles & responsibilities of “DR Team Members”
3. Define Schedules for Training and Mock Testing, and training requirements.

Definition:

A 'disaster / interruption' is defined as the unplanned loss of processing capability due to one or more of the critical assets (hardware / software) going down, for any reason, exceeding pre-determined amount of time. During these times, service delivery would be interrupted.

Minimum Allowable Downtime defined for Critical Devices at Copal Research varies from 2 hours to 48 hours for different business functions. This is as per the Business Impact Analysis sheet.

Downtime of greater than pre-determined allowable outage time for the respective business function is defined as 'Disaster', and the recovery procedures would come into effect.

Resumption of time-sensitive business operation is dependent on availability of the resources required to support the associated functions and processes. This would be defined in the various disaster recovery procedures to be carried out.

Management Priorities:

Ensure that the critical business processes and information assets that are required to support the business are identified and classified. The classification should be as follows:

- Core Business Functions
- Primary Supporting System
- Key Personnel
- Maximum Tolerable Downtime

1.2 SCOPE AND PURPOSE

Given the broad range of IT designs and configurations as well as business dynamics, as well as the rapid development and obsolescence of products and capabilities, the scope of this
document is to define practices for applying technology to enhance an organization's contingency planning capabilities.

Scope Includes:

- Devices/ Services

The Scope of this document is to cover all the Information Technology Components and IT driven systems that are:

- Devices as identified in the Asset Register
- To be profiled for recovery
- Incident Type

The document outlines planning principles applied to a wide variety of incidents that could affect IT system operations.

- Software
- Application Crash
- Operating System Problem
- Hardware Problem of Critical Servers
- LAN Unavailable

- WAN Unavailable
- Human Threats

1.3 AUTHORIZATION

The Copal Research DR team has developed this document. The guidelines specified in this document are to be followed by all the business units of Copal Research.

The Recovery Teams/DR Head can suggest changes to the DR.

The final approval of the changes required will be of DR Head in consultation with the Information MISF.

1.4 AUDIENCE

Individuals responsible for security at system and operational levels can use the principles presented in this document. This description includes the following personnel:

Managers:
Responsible for overseeing operations or business processes which rely on IT

Systems.

System Administrators:
Personnel responsible for the management of daily IT operations.

System Developers and Architects:
Responsible for designing, implementing, or modifying information systems applications.

Users:
Responsible for using desktop and portable systems to perform their assigned job functions.

Other personnel:
Responsible for designing, managing, operating, maintaining, or using Information systems.

1.5 KEY ASSUMPTIONS

The following assumptions have been established as the basis for the development of the Disaster Recovery Plan:

- The plan is designed to recover from the "worst case" disruptions of Copal Research's operating environment. The worst case excludes any

non-data processing function that may be in close proximity to the server room or workstations.

- The level of detail of the plan is written to a staff experienced in Copal Research's computer services. It assumes that at the time of disaster development, testing and implementation of new technologies and applications are suspended so that all resources are available to recover existing critical production processing.
- As some of the critical devices, do not have stand-by arrangements in place, off-site inventory and equipment acquired through vendors is considered to be the only resource with which to recover computer processing.
- An alternate site (backup computer facility) in which to establish recovery of computer processing is necessary. If necessary non-core functions can be outsourced till the business returns back to normal condition.
- The current plan assumes that personnel of Copal Research are always able to reach office premises. Unavailability of personnel due to natural or other calamities is not considered within this document as a disaster if the IT facility being monitored for disaster is fully operational with all systems online.

Disaster Probability Matrix:

The disaster probability matrix is created on the basis of:

- History data of such incidents
- Any ongoing incidents during the execution of the plan and/or testing, which has an impact on, the probability assumed.

Type of Disaster	Assumed Probability
Software o Application Crash o Operating System Problem	Once in 3 months
Hardware Problem of Critical Servers	Once in 6 months
LAN Unavailable	Once a year
WAN Unavailable	Once a year
Human Threats	Once a year
Environmental Threats :Full site shutdown due to Fire , Floods, electricity break out etc.	Once a year

The Disaster recovery plans for the above threats are mentioned in the Disaster recovery strategy document.

1.6 DOCUMENT STRUCTURE

This document is designed to logically lead through the process of Disaster Recovery. This includes the process of evaluating the organization's needs against recovery strategy options and technical considerations, and documenting the recovery strategy into DR plan. The DR plan and corresponding recovery procedures would serve as a "user's manual" for executing the strategy in the event of a disruption.

The remaining sections of this document address the following areas of DRP:

Section 2, DR Organization:
Details the DR Organization chart and the formation of recovery teams. The section also discusses the roles and responsibilities commonly assigned to team personnel.

Section 3, Business Impact Analysis:
Provides background information about contingency planning, including the purpose of contingency plans and how these plans are integrated into an organization's risk management. It also provides the list of critical assets and recovery priority.

Section 4, Recovery Strategy:
Details the Plan testing and exercises necessary for developing an effective DR Plan. The section presents contingency planning guidance for all elements of the planning cycle, including alternate site selection and recovery strategies.

Section 5, DR Administration:
Describes the distribution of the DR Plan, maintaining, testing, training, and executing the contingency and recovery plan.

2 DR ORGANIZATION

2.1 DR ORGANIZATION CHART

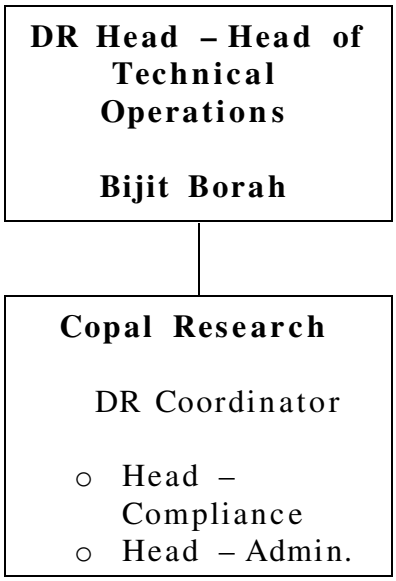
Copal Research is present at the following location:

- 6th Floor, Vatika Atrium, Gurgaon.

Organization structure at Copal Research for DR is defined:

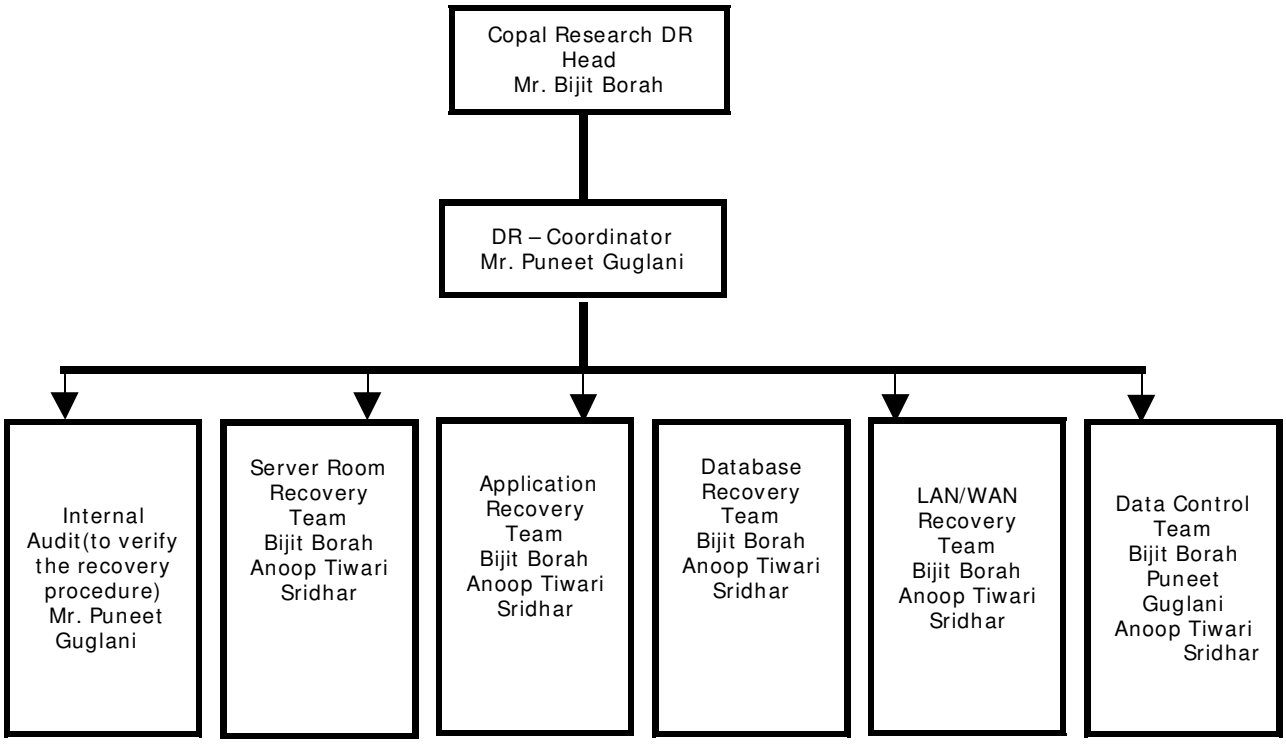
- Function wise (Refer “Figure 2.1” & “Figure 2.2”).

FIGURE 2.1 DR Responsibility Structure



Primary responsibility of DR is of DR Coordinator. The current designated DR Coordinator is Mr. Puneet Guglani and Mr. Rajesh Sandheer. Care should be taken that at least one of the coordinators is reachable and able to take charge either remotely and/or take charge in minimum 30 minutes, depending on the function that has gone down. The maximum downtime allowed for the most critical function is 2 hours, and hence the need to take charge within at least 30 minutes.

FIGURE 2.2 Organizational Chart- Function wise



- All the teams will be supported by the data control team, this team is responsible for media protection and backup at Copal Research.
- The teams would be staffed with a mix of Copal Research employees and outsourced vendor teams, as required.

2.2 DR TEAM

The DR team has been formulated with following considerations.

- Skills / Knowledge Possessed by the Team Members
- Previous knowledge of same function
- Training on Contingency Plan purpose
  - Training on Various Procedures for executing the recovery plan

Each team has as such only one person. Also, the person is responsible for multiple functions with core competency in at least one. There are at least two persons identified per team, to take care of the non-availability of person issues.

Line of succession planning is included in the DR. The order of succession will define who assumes responsibility for DR execution. The line of succession ends at the alternate DR Coordinator. Personnel lower than the DR Coordinator should not be vested with authority powers to invoke "crisis / recovery", since they may panic and initiate recovery procedures without doing a proper assessment, thereby creating chaos. Copal Research has to ensure availability of DR Heads and/or DR Coordinators.

Following issues should be considered in case of disaster:

- The possibility of a disaster should be considered that would render a majority or all personnel unavailable to respond. Such an event is a likely occurrence when there is a communication links failure, Act of GOD, Manmade disasters like Fire in the entire facility have been considered in the document.

- IT Staff consists of few people at Copal Research. In such cases, it is not possible to have separate teams staffed for separate functions. Keeping this in mind, we recommend having teams, which perform multifunctional roles, with a core competency in at least one area.

- Since it is not possible to have staff additions due to low requirements, we recommend having priority driven SLAs with vendors. Copal Research should have contracts, which ensure they get priority over others for events Copal Research defines as disaster. This is also required since Copal Research does not stock any spare equipment. Priority driven SLAs would ensure Copal Research gets priority for certain events pre-defined and qualified as disaster by Copal Research. These could be specific event based priced events rather than a huge one time premium cost. These vendors can be called upon from anywhere by DR coordinators or DR heads to ensure successful recovery procedures for hardware failures.

- It is possible that the vendor may run out of resources considering the disaster scenario, having SLA with the vendor will help to ensure the help when required most.

DR Teams:

The DR team at the various locations has been defined as follows

Table 2.1 – Personnel Identified for Disaster Recovery Management.

Network Recovery Team			
	Vatika Atrium Facility	LAN Recovery Team	Mr. Anoop Tiwari

	Vatika Atrium Facility	Network OS Team	Mr. Anoop Tiwari
	Vatika Atrium Facility	Desktop Support Team	Mr. Anoop Tiwari
Internal Audit Team			
	Vatika Atrium Facility		Mr. Puneet Guglani
Center Recovery Team (AC, fire, building etc.)			
	Vatika Atrium Facility	Electric Team	Mr. Rajesh Sandheer Mr. Surinder Choudhary
	Vatika Atrium Facility	Fire Safety Team	Mr. Rajesh Sandheer Mr. Surinder Choudhary
Application Recovery Team			
	Vatika Atrium Facility	Application Team	Mr. Anoop Tiwari Mr. Bijit Borah
	Vatika Atrium Facility	Database Recovery Team	Mr. Anoop Tiwari Mr. Bijit Borah
	Vatika Atrium Facility	Data Control Team	Mr. Anoop Tiwari Mr. Bijit Borah

2.3 DR ROLES AND RESPONSIBILITIES

DR Coordinator: (**Refer Table 2.1** for Individuals allocated in the team)
DR Coordinator for a location is responsible for executing DR at the location. Overall responsibilities of the coordinator include: o Damage Assessment in case of a disaster o Declaration of the disaster o Communication to the DR Head o Recovery Team Formation o Recovery Teams Coordination o Monitoring the recovery process and communicate the same to DR Head The DR Coordinator must designate appropriate teams to implement the strategy. • Each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation. • Every recovery team member need to clearly understand o Team's goal in the recovery effort o Each step required to be executed o Inter-dependence on other teams o The size of each team, specific team titles, and hierarchy designs depend on the organization.

DR Teams – Roles & Responsibilities

LAN/WAN/Desktop/Server Recovery Team

Includes
--Desktop Recovery
--Network Recovery (includes Physical links, network equipment)
--Server Recovery
--Email Recovery

Responsibilities:

- Obtaining authorization to access damaged facilities
- Damage Assessment
- Restoring network to normal condition
- Allowing network users access to networked services
- Connecting network to other external systems
- Obtaining necessary office supplies and workspace
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media. Backup media to be obtained for applications from the Data Control Team.
- Restoring critical operating system and application software
- Restoring system data
- Assessing the required OS recovery measures
- Execution of the steps based on the installation checklist
- Restoring Telecommunication facilities to normal working conditions
- Coordination with vendor for restoration of telecom links.
- Provide necessary hardware/software support during the telecom restoration process

Administrative Team

Includes
Electric Team (Mr. Rajesh Sandheer and Mr. Surinder Chaudhary)
Fire Safety Team (Mr. Rajesh Sandheer and Mr. Surinder Chaudhary).

Responsibilities:

- Obtaining authorization to access damaged facilities
- Damage Assessment of electrical equipments.
- Restoring electric facilities back to normal operating conditions
- Maintaining proper documentation of the available fire infrastructure
- Vendor coordination
- Testing of fire equipment on periodic basis.

Software Recovery Team

Includes Data Control Team, Application Recovery Team and Database Recovery Team

Responsibilities

- Restoration based on the Damage Assessment results and installation checklists
- Obtaining authorization to access damaged facilities
- Restoring Databases and applications based on databases
- Maintain documentation of the databases and their connectivity to other applications/databases
- Maintain documentation of the database-based applications
- Restoration based on the installation checklists
- Troubleshooting
- Provide hardware/system level support for the database restoration process

Pre-Requisites for the team

The teams defined above need to be:

- Well-versed with recovery procedures.
- Trained and fully equipped to handle situations.
- Trained in soft skills also. They should know what information can they divulge and what not. Also, what kind of information to divulge to personal relations.
- When and who should communicate with the outside world? The outside world could be Press, friends etc.
- The teams should be technically competent, and very well versed with the procedures and checklists to be followed.
- They should know when their role in the process starts and ends.

3 BUSINESS IMPACT ANALYSIS

The Business Impact Analysis (BIA) is a key step in the Continuity Management process. The BIA enables the DR Coordinator to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The purpose of conducting a BIA is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's DR Plan.

3.1 CONTINGENCY PLANNING AND RISK MANAGEMENT PROCESS

Process Description:

Risk management encompasses a set of activities to identify, control, and mitigate risks to an IT system.

In the Risk assessment process carried out by Risk Assessment Team, threats and vulnerabilities existing in the systems were identified so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident.

- Type of threats addressed:
- Natural - e.g. hurricane, tornado, flood, and fire
- Human - e.g. operator error, sabotage, implant of malicious code, and terrorist attacks

- Environmental - e.g. equipment failure, software error, and telecommunication network outage and electric power failure.
- Identifying and documenting residual risks for which contingency plans must be put into place.
- A thorough risk assessment was conducted to identify:
- Risks / threats
- Current controls in place
- The likelihood of occurrence and its impact

Because risks can vary over time and new risks may replace old ones as a system evolves, the risk management process must by ongoing and dynamic. Risk assessment activity should be carried out on a periodic basis (once in 6 months)

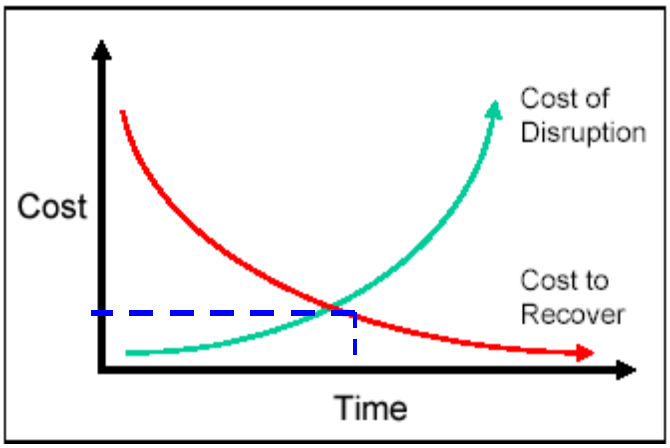
Responsibility:

The Recovery Teams should carry out the Risk Assessment activity and findings should be conveyed to the DR Coordinator.

3.2 KEY LOCATIONS/ KEY PROCESSES AND CLASSIFICATION

The matrix given below (Table 3-3) explains Copal Research's key locations with recovery priority and the critical time frame. The optimum point to recover the IT system by balancing the cost of system inoperability against the cost of resources required for restoring the system. This can be depicted using a simple chart, such as the example in Figure 3-2. The point where the two lines meet will define how long the organization can afford to allow the system to be disrupted.

Figure 3-2 Recovery Cost Balancing



As of this document, we have used assumptions and qualitative analysis to arrive at allowable outage times of business functions and the recovery strategy.

The assumed allowable outage time for key business processes are defined in the Table 3-3 Criticality Matrix. These outage times need to be defined by Business Heads.

This information is used as a base for defining “disaster “and recovery strategy.
Since allowable downtime is in the range of 2 – 48 hours, recovery strategy, along with a base line, would be different for different applications; depending on the allowable outage times.

Dotted blue lines in the above figure show Copal Research’s Cost-Recovery estimate.

Key Processes and Allowable outage times
The Key functions at Copal Research and allowable outage time for key business processes are defined in the Table 3.3 Criticality Matrix.

Table 3.3 Criticality Matrix

Priority	Function	Allowable Outage Time
1	Windows based File server	2 hours
4	Mailing & Messaging Services Maintenance	4 hours
3	Server Backup Services	2 hours
2	IT Infrastructure (LAN/ WAN)	2 hours

The processes listed above include Helpdesk, Backup, Vendor Management, Training as sub-processes thereby having the same allowable outage times as the primary processes.

From the list of functions listed above, we conclude the following:

- Priority defined here is the sequence in which the applications need to be brought back up in case of a disaster.

4 RECOVERY STRATEGY

One of the most important aspects of Disaster Recovery Planning for the majority of organizations is in choosing an appropriate strategy for the back up and recovery of the IT based systems.

The key business processes are matched against the IT system and an appropriate speed of recovery strategy is chosen.
Parameters considered while developing the strategy include:

1.1. Critical Assets
1.2. Allowable outage time
1.3. Operational requirements of Copal Research
1.4. Cost
1.5. Commercial contracts with alternate site vendors
1.6. Service level agreements (SLAs) with the equipment vendors
1.7. Power supply Backup (UPS, etc.)
1.8. Off-site Backup Media Storage

As listed in Table 3.3 Criticality Matrix, allowable downtime varies in the range of 2 hours to two-days.

Based on the current state assessment, the planning and groundwork required for Recovery Strategy suggested for Copal Research is as follows:

1.1. Critical Assets Identification and Retrieval Process Documentation. These should be documented and reviewed for changes every 3 months.
1.2. Back up Process based on the criticality of the systems/application. These should be reviewed every 3 months.
1.3. Restoration testing of backup tapes should be done every month.
1.4. DR Organization Structure with well-defined roles and responsibilities. The resources should be trained adequately and skilled in all aspects.
1.5. Testing of the DR processes to be carried out as classroom at least every two months, and actual drills every three months.
1.6. Modification if required after the testing phase

A Budget Plan for DR now needs to be prepared. The Budget Plan takes into account costs occurring under various heads. Costs can be one-time investment or they can be recurring in nature. The Budget Plan should be reviewed and updated on a regular basis.

4.1 RECOVERY STRATEGY AND PLAN

4.1.1 PRE-REQUISITES

- Business functions once defined as DR critical and non critical are segregated. We now undertake to build recovery procedures first for the DR critical functions, and within this list we start by taking the most critical functions, sorted on least allowable outage times.
- The next step is to identify IT functions, which the business functions use. Here, we restrict ourselves to those IT functions, which are present in the server room. The IT functions here would include server related functions, application interface, and database functions. Essentially, we cover access to the server/network devices and the applications running on them throwing information back to the users.
- This means as of now, we have the following defined:
    - Business Function
        - Dependent IT function in server room
            - Dependent IT asset in the server room
            - Allowable outage time for each asset based on its relationship with the business function
            - Identified dependencies and common assets in use in the IT functions, e.g. network devices, shared databases, e-mail etc.

4.1.2 STRATEGY

Pre-Requisite:

Operations:

- The DR Strategy exists undertakes the resource level redundancy & recovery practices at the Primary Site. As per Management Decision, plans will be developed for Site level redundancy at alternate location.

Technology:

- Keep a OS recovery tape , this is a disk image of the hard disk on which the OS is loaded.
- Keep redundant configurations in the hardware itself, i.e. dual Ethernet card, dual power supply, mirrored hard disks, RAID for database hard disk, Cluster
- Keep spares on site so that they could be used instantly to replace the faulty set
- The RAID/Cluster facility on the server would help us recover from data losses.
- The tape backup contains incremental data of one day

- Keep a DR tape, with the database data and OS data at an offsite location
- People are trained in DR procedures and techniques.
- Redundant links from ISP physical (two leased circuits) and logical(two ISPs)

The plan is to:

- Analyze the incident
- If site failure, identified personnel to be carried to alternate site for working from there. This is to be done by way of Copal Research transport.
- If hardware failure, we have redundant systems internally that take over while we replace using onsite spares
- If software failure, we have OS and database recovery tapes which immediately can be used to restore.
- If data communication links failure, we have redundant devices and links that can take over.

4.2 COMMUNICATION TO THE MEDIA

In case of a disaster, reputation of the company should be safeguarded. Only the head-Corporate Communications of Copal Research is authorized to communicate to the media. All other Copal Research employees shall refrain from disclosing any information in this regard.

4.3 RISK MITIGATION

The below mitigation measures which would enable us to reach the recommended Backup Strategy for Copal Research

- Giving insurance cover for the critical assets can cover major portion of the risks.
- Engineers/specialists from the vendors such as Microsoft, hardware vendors should be included in the recovery teams discussed. This way, Copal Research would not need to increase internal headcounts while ensuring timely recovery.
- An NDA should be signed with all personnel who have access to classified data/information.
- Schedule for restorability testing of backup tapes
- Keep one backup as a snapshot of OS, Application, and Databases. These would be labeled as DR tapes to be used first for recovery before inserting any weekly or daily data backup tapes.

- We need to put definite times to our procedures. For processes such as backup and restore, we need to ensure they finish within definitive timelines. Any deviation from the timelines should be viewed seriously and recorded for further investigation.
- All incidents, small and big, should be recorded in a formal incident response form in accordance with the Incident Response Security Policy.

4.4 PLAN TESTING AND EXERCISES

Plan testing is a critical element of a viable DR capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each DR element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

The basic format for DR test is

Classroom Exercises:

Participants in classroom exercises, often called tabletop, walk through the procedures without any actual recovery operations occurring. Classroom exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise.

Guidelines for Classroom Exercises:
Develop and conduct plan exercises. Exercises will grow in complexity over time. Include announced and unannounced events.

- Document the objectives for each exercise. Individual objectives should include responsibility assignments and measurement criteria.
- Evaluate the results of each exercise against pre-stated measurement criteria and document results along with proposed plan enhancements.
- Emergency response exercises should be ongoing, quarterly events using alternate scenarios and should involve every organization within a particular facility that may be affected by a system disaster.
    - Exercises can be conducted in phases such as
        - Phase 1: First-level activation of the continuity plan:
          - Initial damage assessment and reporting the findings to the Team for use in decision-making
        - Phase 2 – Walkthrough of checklists for restoration of critical devices and off-site backup arrangements. In this phase logistics procedures can be verified and noted.

To derive the most value from the test, the DR Coordinator should develop a test plan designed to test the selected element(s) against explicit test objectives and success criteria. The test plan should include a schedule detailing the time frames for each test and test participants. The test plan should also delineate clear scope, scenario, and logistics. The scenario chosen may be a worst-case incident or an incident most likely to occur. It should mimic reality as closely as possible.

It is important that an exercise must never disrupt normal operations. If testing at the alternate facility, the DR Coordinator should coordinate test dates and operations with the facility. Test results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan.

4.5 TRAINING OF DR TEAM

It is very important that IT department members know about operations which are not covered in their regular job responsibilities. The training should be carefully planned and delivered on a structured basis. Training may be delivered either using in-house resources or external resources depending upon available skills and related costs.

A skill matrix of Copal Research IT staff members is to be maintained. The skill matrix summarizes resources available in various categories and their skill level.

Objective:

Resources identified in different categories can be given some training so that they can start the recovery procedures before getting support from vendor or other locations.
Developing expertise for the recovery of critical systems identified at Copal Research. Recovery Teams should be aware of systems recovery process flow at other locations.

Scope:

IT Staff Members identified in Recovery Teams to be trained. Also an agreement regarding the confidentiality of Copal Research data should be signed with them.

Training Needs Assessment:

The plan must specify which person or group of persons requires which type of training

Training Materials Development Schedule:

Once the training needs have been identified it is necessary to specify and develop suitable training materials. This can be a time consuming task and unless priorities are given to critical training program, all the DRP areas will not be covered.

5 DR PLAN MANAGEMENT AND ADMINISTRATION

DR Plan Administration is the responsibility of a designated individual, such as a DR Coordinator. As the custodian and administrator of the Business Contingency Plan, the DR Coordinator must have a thorough knowledge of all Plan contents. Responsibility for maintaining specific sections of the Plan resides with each Team Leader in accordance with the Team's objectives and functional responsibilities of Response, Resumption, Recovery and Restoration.

Should a plan review necessitate any changes or updates, the DR Coordinator is responsible for generating the changes and issuing the updates. The changes made in the DR Plan must be recorded in accordance with a strict version control mechanism. Individuals in responsible Management positions will be called upon periodically to provide information necessary for maintaining a viable plan and exercised recovery capability. Cooperation in the endeavor is essential.

5.1 DR - HEAD

An overall DR Head should be appointed who reports directly to the management team responsible for DR. This person is ideally someone who understands the business processes of the organization and people.

5.2 DISTRIBUTION OF THE DR PLAN

The Copal Research DR Plan is a restricted document, since it contains Proprietary Information. This document is classified as **Confidential**. This plan is also restricted since it contains the Copal Research's strategy for recovery of business critical assets.
Hence the plan should be distributed on a **need-to-know** basis. Each individual possessing a copy of the DR Plan is responsible for the protection of the same. A list of these names should be maintained.

5.3 MAINTENANCE OF THE DR PLAN

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists

At a minimum, plan reviews should focus on the following elements:

- Operational requirements
- Security requirements
- Technical procedures
- Hardware, software, and other equipment (types, specifications, and amount)

- Names and contact information of team members
- Names and contact information of vendors, including alternate and off-site vendors
- Alternate and offsite facility requirements
- Vital records (electronic and hardcopy).

Because the DR Plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. A copy of the plan should also be stored at the alternate site and with the backup media to ensure its availability and good condition in case of the disaster.

The DR Coordinator should maintain a record of copies of the plan and to whom they were distributed. Other information that should be stored with the plan includes:

- contracts with vendors (SLAs and other contracts),
- software licenses,
- system users manuals,
- security manuals, and
- operating procedures.

The DR Coordinator should record plan modifications using a Version Control Maintenance Form, which lists the Serial number, Description of Change, Date of Change, Name & Signature of the person by whom it is reviewed, Name & Signature of the person by whom it is approved and the Date of Issue. Strict version control must be maintained by requesting old plans or plan pages to be returned to the DR Coordinator in exchange for the new plan or plan pages.

The DR Coordinator should also review following supporting information to ensure that the information is current and continues to meet system requirements adequately:

- Alternate site contract, including testing times
- Off-site storage contract
- Software licenses
- MOU or vendor SLA
- Hardware and software requirements
- System interconnection agreements
- Security requirements

- Recovery strategy

- Contingency policies
- Training and awareness materials
- Testing scope.

Although some changes may be quite visible, others will require additional analysis.
The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities.

A structured and controlled DR updating process will involve the use of formalized change control procedures under the control of the DR Team Head.

- **Change Control Procedures for Updating the Plan**
- **Responsibilities for Maintenance of Each Part of the Plan:** Each part of the plan will be allocated to a member of the DR Team or a Senior Manager with the organization who will be charged with responsibility for updating and maintaining the plan.
- **Testing Responsibility:** The DR Team will nominate one or more persons who will be responsible for co-coordinating all the testing processes and for ensuring that all changes to the plan are properly tested.

People Continuity Structure

Sr. No.	Primary Role	Supporting Personnel's	
		Administrative	*Operational*
1	Sr. VP – Ops	Head - IT, Head – Compliance	Head – IT, Head – Compliance
2	Head –IT	Sr. VP – Ops	Systems Engineer
3	Head –Compliance	Sr. VP – Ops	Head – IT, Head – Administration, Systems Engineer
4	Head – Administration	Sr. VP – Ops	Manager – Administration
5	Manager – Administration	Head – Administration	Head – Administration
6	Systems Engineer	Head – IT	Head – IT, Head – Compliance.

APPENDIX E:

9.1c Disaster Recovery Framework

Copal Partners

Document Revision History

Version	Date	Author(s)	Revision Notes	Approved by

Distribution List

1. Head – India
2. Sr. VP – Operations
3. Head - IT
4. Head – Compliance
5. Head – Administration.

Disclaimer

Version: 1.0

Author: Erik Simonsen, SVP, Operations

Approved by: Aman Chowdhury, Country Head - India

Last updated: 12 May, 2006

Issue Date: 12 May, 2006

Effective Date: 12 May, 2006

Purpose

This document outlines the Business Continuity and Disaster Recovery Management Procedures for Copal Research.

Objectives

The objectives of the Disaster Recovery Framework are to:

- Develop a cost-effective framework for the resumption of services after a business interruption.
- Define Roles & responsibilities of the DR Team Members
- Define Schedules for Training and Mock Testing, and training requirements.

List of Critical Systems, and Associated Service Risks

This Document applies to all business functions and information systems in Copal Partners' facilities in India. The tables below summarize the categories of these systems, and present an indicative list of respective business-critical incidents.

Critical Systems

This document covers all business-critical IT Components and IT-driven systems, including:

IT Infrastructure Component	Sub Component
LAN	Desktops / Laptops
	L2 switches or user-level network failure
	DMZ
	Firewalls
	Backbone including Layer 3 Switch
WAN	Site-to-Site Connectivity
	WAN Routers
	Internet access/Proxy Services
Domain Infrastructure	Domain Controllers/DNS
	DHCP
E-Mail	Mail Servers
	Virus Walls
Voice Communication	Phones
	e PBX
File / Print servers	Corporate (Finance, Administration, HR etc.)
	Delivery
Software	Operating systems - Client
	Operating systems – Server
	Corporate applications
	Business tools

Service Risks Probabilities

The document outlines planning principles applied to a wide variety of incidents that could affect IT system operations. These risks are categorized by probability and severity of occurrence, and form the basis for the business impact and recovery procedures in BCM documentation.

Risk Type	Probability	Severity
Virus attack	3	2
Security breaches	2	3
ISP failure	2	3
Unavailability of critical records or media	2	2
Accidental deletion of critical data	2	2
Total facility outage	1	3
Utility outage (Power, A/C etc)	1	3
Unavailability of key staff	1	2
Lack of spares (hardware, etc)	1	2
System / Equipment Failure	1	2
Human Error	1	1

Note: Probability and Severity have been assigned by the schedule below based on historical or estimated frequency and impact.

Probability	Approximate Frequency	Severity	Business Impact
0	Once in 5 years	0	Not Serious
1	Once per year	1	Moderately serious – Affecting one user or a group of users for half a day or less
2	Once per quarter	2	Serious – Affecting an entire team or process
3	Up to once per quarter	3	Catastrophic – Service delivery is affected across the facility

Change Management

The Copal Research DR Team has developed this document. The guidelines specified in this document are to be followed by all business units of Copal Research.

The Recovery Teams/DR Head can suggest changes to the DR.

Changes may only be ratified by the DR Head in consultation with the Copal Management of Information Security Forum. Changes are subject to Copal's standard document management procedures. The DR Head is the owner of these documents.

Key Assumptions
Definition of Disaster

In this document, a disaster is defined as the unplanned loss of processing capability due to the loss or malfunction of one or more of the critical systems, resulting in impaired service delivery.

Minimum Allowable Downtime

The Minimum Allowable Downtime defined for critical services at Copal Research varies from 2 hours to 48 hours for different business functions, according to a Business Impact Analysis Matrix.

Any downtime of greater than pre-determined Minimum Allowance respective business function is defined as 'Disaster', and trigger recovery procedures.

Recovery Procedures and Requirements

Recovery procedures for each role and process are described in Business Continuity Procedure documents unique to each business function.

As a general guideline, any event that impacts client service delivery for over two hour is classified as a disaster, and operations must be restored to a minimum of 20% capacity within 4 hours.

Document Structure

This document is designed to logically lead through the management process of Disaster Recovery. This includes the process of evaluating the organization's needs against recovery strategy options and technical considerations, and documenting the recovery strategy into DR plan. The DR plan and corresponding recovery procedures would serve as a user's manual for executing the strategy in the event of a disruption.

The remaining sections of this document address the following areas of DRP:

- **Section 2, DR Organization:** Details the DR Organization chart and the formation of recovery teams. The section also discusses the roles and responsibilities commonly assigned to team personnel.

- **Section 3, Business Impact Analysis:** Provides background information about contingency planning, including the purpose

of contingency plans and how these plans are integrated into an organization's risk management. It also provides the list of critical assets and recovery priority.

- **Section 4, Recovery Strategy:** Details the Plan testing and exercises necessary for developing an effective DR Plan. The section presents contingency planning guidance for all elements of the planning cycle, including alternate site selection and recovery strategies.

- **Section 5, DR Administration:** Describes the distribution, maintaining, testing, training, and executing of the contingency and recovery plan.

DR Organization
DR Facilities

Copal Research is present at the following locations:

Site 1: 6th Floor, Vatika Atrium, DLF Golf Course Road, Sector 53, Gurgaon, Haryana 122002 India

Site 2: 6th Floor, Vatika Atrium, DLF Golf Course Road, Sector 53, Gurgaon, Haryana 122002 India

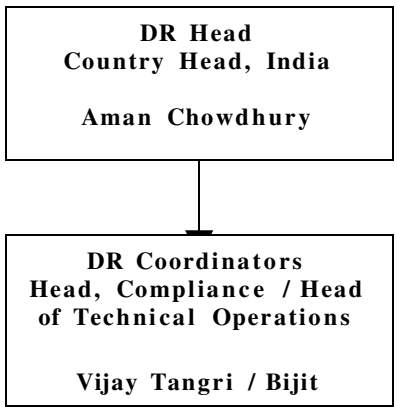
Each site contains sufficient hot or warm spare seats support a minimum of 20% of the operations of the other site in case of a site-wide disaster. These spare areas include all facilities required for process failover, including desktop PCs, printers/scanners, data sources, internet/telecom facilities, shredders, access-controlled areas, and servers. Business critical file systems from one site are mirrored to hot-standby servers at the other site in real time.

DR Organization Structure

The DR Organization structure at Copal Research can be defined by BCM responsibility or by process responsibility. The BCM process owners are responsible for ensuring the development, maintenance, testing, and improvement of the BCP and DR documentation. Process owners are responsible for the maintenance and—in the case of disaster—restoration of business continuity plans.

BCM Responsibility Structure

FIGURE 2.1 BCM Responsibility Structure



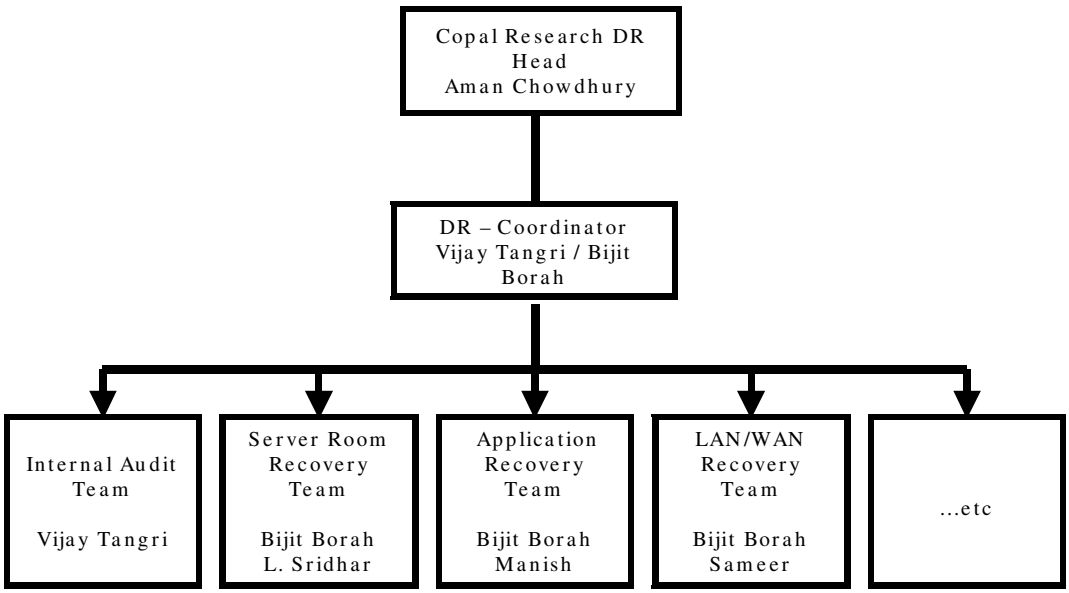
The DR Coordinator has the primary responsibility of DR execution. The current designated DR Coordinators are Vijay Tangri and Bijit Borah. Care should be taken that at least one of the coordinators is reachable and able to take charge in a minimum 30 minutes from the recognition of a disaster. The maximum downtime allowed for the

most critical function is 2 hours, and hence the need to take charge within at least 30 minutes.

DR Process Teams

The Process teams each have a designated leader and a backup, where appropriate. Process teams are responsible for the planning and execution of business recovery procedures for their functional domain.

FIGURE 2.2 BCM Process Responsibility Chart



The DR teams at the various locations has been defined as follows

Network Recovery Team		
Vatika Atrium Facility	LAN Recovery Team	Bijit Borah/ L.Sridhar
Vatika Triangle Facility	LAN Recovery Team	Mahender Singh
Vatika Atrium Facility	Network OS Team	Bijit Borah/ L. Sridhar
Vatika Triangle Facility	Network OS Team	Sameer Chaudhary
Vatika Atrium Facility	Desktop Support Team	Mahender Singh
Internal Audit Team		
Vatika Atrium Facility	Internal Audit Team	Vijay Tangri

Facility Recovery		
Vatika Atrium Facility	Electric Team	Amandeep Singh
Vatika Triangle Facility	Electric Team	Anil Dalal/ Amandeep Singh
Vatika Atrium Facility	Fire Safety Team	Surinder Chaudhary/ Anil Chauhan
Vatika Triangle Facility	Fire Safety Team	Anil Dalal
Application Recovery		
Vatika Atrium Facility	Application Team	Bijit Borah
Vatika Triangle Facility	Application Team	Manish Bhatia
Vatika Atrium Facility	Database Recovery Team	Bijit Borah/ L. Sridhar

DR Roles and Responsibilities
BCM Roles

DR Head: (**Refer Table 2.1** for Individuals allocated in the team)

DR Head bears ultimate responsibility for the DR process.

Overall responsibilities of the head include:

- Oversight of the Business Continuity Management and Planning Processes.
- Ratification of documentation and plans.
- Selection and management of the DR Coordinator

DR Coordinator: (**Refer Table 2.1** for Individuals allocated in the team)

DR Coordinator for a location is responsible for executing DR at the location.

Overall responsibilities of the coordinator include:

- Damage Assessment in case of a disaster
- Declaration of the disaster
- Communication to the DR Head
- Recovery Team Formation
- Recovery Teams Coordination
- Monitoring the recovery process and communicate the same to DR Head

The DR Coordinator must designate appropriate teams to implement the strategy.

- Each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation.
- Every recovery team member need to clearly understand
- Team's goal in the recovery effort
- Each step required to be executed
- Inter-dependence on other teams
- The size of each team, specific team titles, and hierarchy designs depend on the organization.

Process Roles

LAN/WAN/Desktop/Server Recovery Team

Functional Areas include:

- Desktop Recovery
- Network Recovery (includes Physical links, network equipment)
- Server Recovery
- Email Recovery

Responsibilities

- Obtaining authorization to access damaged facilities
- Damage Assessment
- Restoring network to normal condition
- Connecting network to other external systems
- Obtaining necessary office supplies and workspace
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media. Backup media to be obtained for applications from the Data Control Team.
- Restoring critical operating system and application software
- Restoring system data
- Assessing the required OS recovery measures
- Execution of the steps based on the installation checklist
- Restoring Telecommunication facilities to normal working conditions
- Coordination with vendor for restoration of telecom links.
- Provide necessary hardware/software support during the telecom restoration process

Administrative Team

Functional Areas include:

- Electric Team
- Fire Safety Team

Responsibilities

- Obtaining authorization to access damaged facilities
- Damage Assessment of electrical equipments.
- Restoring electric facilities back to normal operating conditions
- Maintaining proper documentation of the available fire infrastructure
- Vendor coordination
- Testing of fire equipment on periodic basis.

Software Recovery Team

Functional Areas include:

- Application Recovery Team
- Database Recovery Team

Responsibilities

- Restoration based on the Damage Assessment results and installation checklists
- Obtaining authorization to access damaged facilities
- Restoring Databases and applications based on databases
- Maintain documentation of the databases and their connectivity to other applications/databases
- Maintain documentation of the database-based applications
- Restoration based on the installation checklists
- Troubleshooting
- Provide hardware/system level support for the database restoration process

Team Requirements

The teams defined above need to be:

- Well-versed with recovery procedures.
- Trained and fully equipped to handle situations.
- Trained in soft skills. They should know what information can they divulge and what not. Also, what kind of information to divulge to personal relations.
- The teams should be technically competent, and very well versed with the procedures and checklists to be followed.
- They should know when their role in the process starts and ends.

Business Impact Analysis

The Business Impact Analysis (BIA) is a key step in the Continuity Management process. The BIA enables the DR Coordinator to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The purpose of conducting a BIA is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's DR Plan.

Contingency Planning and Risk Management Process Process Description

Risk management encompasses a set of activities to identify, control, and mitigate risks to an IT system.

In the Risk assessment process carried out by Risk Assessment Team, threats and vulnerabilities existing in the systems were identified so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident.

Type of threats addressed:

- Natural - e.g. hurricane, tornado, flood, and fire
- Human - e.g. operator error, sabotage, implant of malicious code, and terrorist attacks
- Environmental - e.g. equipment failure, software error, and telecommunication network outage
- and electric power failure.

Identifying and documenting residual risks for which contingency plans must be put into place.
A thorough risk assessment was conducted to identify:

- Risks / threats
- Current controls in place
- The likelihood of occurrence and its impact

Because risks can vary over time and new risks may replace old ones as a system evolves, the risk management process must by ongoing and dynamic. Risk assessment activity should be carried out on a periodic basis (once in 6 months)

Responsibility

The Recovery Teams should carry out the Risk Assessment activity and findings should be conveyed to the DR Coordinator.

Key locations/ key processes and classification

The matrix given below (Table 3-1) explains Copal Research's key locations with recovery priority and the critical time frame. The optimum point to recover the IT system by balancing the cost of system inoperability against the cost of resources required for restoring the system.

In this document, we have used assumptions and qualitative analysis to arrive at allowable outage times of business functions and the recovery strategy.

The assumed allowable outage time for key business processes are defined in the Table 3-1 Criticality Matrix. These outage times need to be defined by Business Heads, and are used as a base for defining "disaster "and recovery strategy.

Since allowable downtimes are in the range of 2 – 48 hours, recovery strategies are different across applications, depending on allowable outage times.

Key Processes and Allowable outage times

The Key functions at Copal Research and allowable outage time for key business processes are defined in the Table 3.1 Criticality Matrix.

Table 3.1 Criticality Matrix

Function	Allowable Outage Time
Windows based File server	30 minutes
DHCP	1 hour
Print Services	1 hour
Internet Connectivity/DNS	2 hours
IT Infrastructure (LAN/WAN)	2 hours
Employee Transportation Failure	2 hours
Mailing Services	4 hours
Scanning Services	4 hours
Telephone Failure	6 hours
WAN Links	8 hours
Server Backup Services	24 hours

- **Any sub-processes of the processes above inherit the same allowable outage times as the primary processes.**

Recovery Strategy

One of the most important aspects of Disaster Recovery Planning for the majority of organizations is in choosing an appropriate strategy for the back up and recovery of the IT based systems. The key business processes are matched against the IT system and an appropriate speed of recovery strategy is chosen.

Parameters considered while developing the strategy include:

- Critical Assets
- Allowable outage time
- Operational requirements of Copal Research
- Cost
- Commercial contracts with alternate site vendors
- Service level agreements (SLAs) with the equipment vendors
- Power supply Backup (UPS, etc.)
- Off-site Backup Media Storage

As listed in Table 3.1 Criticality Matrix, allowable downtime varies in the range of 2 hours to one day.

Based on the current state assessment, the planning and groundwork required for Recovery Strategy suggested for Copal Research is as follows:

2. Critical Assets Identification and Retrieval Process Documentation. These should be documented and reviewed for changes every 3 months.
3. Back up Process based on the criticality of the systems/application. These should be reviewed every 3 months.
4. Restoration testing of backup tapes should be done every month.
5. DR Organization Structure with well-defined roles and responsibilities. The resources should be trained adequately and skilled in all aspects.
6. Testing of the DR processes to be carried out as classroom at least every two months, and actual drills every three months.
7. Modification if required after the testing phase

A Budget Plan for DR now needs to be prepared. The Budget Plan takes into account costs occurring under various heads. Costs can be one-time investment or they can be recurring in nature. The Budget Plan should be reviewed and updated on a regular basis.

RECOVERY STRATEGY AND PLAN

PRE-REQUISITES

- We now undertake to build recovery procedures first for the DR critical functions, and within this list we start by taking the most critical functions, sorted on least allowable outage times.

- The next step is to identify the IT functions which the business functions use. Here, we restrict ourselves to those IT functions which are present in the server room. The IT functions here would include server-related functions, application interfaces, and databases. Essentially, we cover access to the server/network devices and the applications running on them throwing information back to the users.

STRATEGY

- Business processes are prioritized as a function of business criticality and the probability and severity of possible incidents to the systems on which they rely.

- Full recovery procedures must be planned and documented for each incident type and for each business critical process and system. These procedures must be tested, and improved on a recurring basis.

- Each incident type must include and action plan, a call tree, and an escalation matrix within the company and with all external organizations (e.g. ISPs) involved in the process.

- Risk mitigation techniques must be used wherever possible to decrease the likely impact of a catastrophic event. Where possible, fully redundant, automatic-failover systems should be employed.

- Data must be preserved in multiple sites and in multiple media, with at least one copy of data always kept off-line.

- Process owners, operations teams, and delivery teams must all be familiar with recovery processes and aware of their roles in the same.

- To ensure process improvement, a proper analysis must follow every incident.

- In case of a disaster, reputation of the company should be safeguarded. Only the President or CEO of Copal Research is authorized to communicate to the media.

RISK MITIGATION

Mitigation methods should be employed wherever possible to decrease the probability of incidents, or to reduce their impact. Lists of mitigation strategies by infrastructure element and incident type is below:

IT Infrastructure Component	Sub Component	Risk Mitigation Strategy
LAN	Desktops / Laptops	Buffer of spares, roaming profiles
	L2 switches or user-level network failure	Buffer of spares, saved configurations
	DMZ	L3-Switch redundancy
	Firewalls	Hot spare redundancy
	Backbone including Layer 3 Switch	XRRP Redundancy
WAN	Site-to-Site Connectivity	VPN failover
	WAN Routers	Buffer of spares, VPN failover
	Internet access/Proxy Services	SLAs/Redundancy
Domain Infrastructure	Domain Controllers/DNS	Redundancy
	DHCP	Redundancy
E-Mail	Mail Servers	SLAs/Relay-server redundancy
	Virus Walls	Redundancy

Voice Communication	Phones	SLAs
	e PBX	SLAs/AMCs
File / Print servers	Corporate	On-site and off-site redundant mirrors, data backups
	Delivery	On-site and off-site redundant mirrors, data backups
Software	Operating systems - Client	Buffer of spare PCs
	Operating systems – Server	Backups, server redundancy
	Corporate applications	Backups, server redundancy
	Business tools	Backups, server redundancy

Risk Type	Risk Mitigation Strategy
Virus attack	Antivirus software in mail/web gateways, on servers, and on desktops; regular verification of updates and monitoring of A/V logs
Security breaches	Regularly monitored firewalls and filtering routers; development of minimum security baseline configurations for all server and network systems.
ISP failure	SLAs with vendors and 50% redundancy
Unavailability of critical records or media	Real time data mirroring on multiple file servers; regular system backups.
Accidental deletion of critical data	Offline staging of deleted items; regular system backups.
Total facility outage	DR site with 20% recovery capacity.
Utility outage (Power, A/C etc)	UPS; DR site with 20% recovery capacity.
Unavailability of key staff	Nominated backups for all critical staff
Lack of spares (hardware, etc)	10% spares policy
System / Equipment Failure	AMCs and SLAs with all vendors, including provision of spare equipment in emergencies; DR site with 20% recovery capacity.
Human Error	Strict implementation of IT

	policies through checklists. Regular training and audit of personnel.

PLAN TESTING AND EXERCISES

Plan testing is a critical element of a viable DR capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each DR element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

Test Format

- Classroom Exercises: Participants in classroom exercises, walk through the procedures without any actual recovery operations occurring. Classroom exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise.
- Document the objectives for each exercise. Individual objectives should include responsibility assignments and measurement criteria.
- Evaluate the results of each exercise against events. Pre-stated measurement criteria and document results along with proposed plan enhancements.
- Emergency response exercises should be ongoing, quarterly events using alternate scenarios and should involve every organization within a particular facility that may be affected by a system disaster.
- Exercises can be conducted in phases such as
    - Phase 1: First-level activation of the continuity plan: Initial damage assessment and reporting the findings to the Team for use in decision-making
    - Phase 2 – Walkthrough of checklists for restoration of critical devices and off-site backup arrangements. In this phase logistics procedures can be verified and noted.
- To derive the most value from the test, the DR Coordinator should develop a test plan designed to test the selected element(s) against explicit test objectives and success criteria. The test plan should include a schedule detailing the time frames for each test and test participants. The test plan should also delineate clear scope, scenario, and logistics. The scenario

chosen may be a worst-case incident or an incident most likely to occur. It should mimic reality as closely as possible.

Test Analysis

- Test results should be documented and analyzed for gaps.
    - Delivery team leads should be interviewed for operations impact
    - Recovery process leaders and teams should report on smoothness of failover and faults in the plan.
    - Recovery times and service levels should be documented, and should be presented along with a summary of recommendations to the MSIF and DR planning committee.

DR Plan Management and Administration

DR Plan Administration is the responsibility of a designated individual, such as a DR Coordinator. As the custodian and administrator of the Business Contingency Plan, the DR Coordinator must have a thorough knowledge of all Plan contents. Responsibility for maintaining specific sections of the Plan resides with each Team Leader in accordance with the Team's objectives and functional responsibilities of Response, Resumption, Recovery and Restoration.

Should a plan review necessitate any changes or updates, the DR Coordinator is responsible for generating the changes and issuing the updates. The changes made in the DR Plan must be recorded in accordance with a strict version control mechanism. Individuals in responsible Management positions will be called upon periodically to provide information necessary for maintaining a viable plan and exercised recovery capability. Cooperation in the endeavor is essential.

Distribution of the DR Plan

The Copal Research DR Plan is a restricted document, since it contains Proprietary Information. This document is classified as **Confidential**. This plan is also restricted since it contains the Copal Research's strategy for recovery of business critical assets.
Hence the plan should be distributed on a **need-to-know** basis.
Each individual possessing a copy of the DR Plan is responsible for the protection of the same. A list of these names should be maintained.

Maintenance of the DR Plan

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. As a general rule, the plan should be reviewed

for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists

At a minimum, plan reviews should focus on the following elements:

- Operational requirements
- Security requirements
- Technical procedures
- Hardware, software, and other equipment (types, specifications, and amount)
- Names and contact information of team members
- Names and contact information of vendors, including alternate and off-site vendors
- Alternate and offsite facility requirements
- Vital records (electronic and hardcopy).

Because the DR Plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled.

A copy of the plan should also be stored at the alternate site and with the backup media to ensure its availability and good condition in case of the disaster.

The DR Coordinator should maintain a record of copies of the plan and to whom they were distributed. Other information that should be stored with the plan includes:

- contracts with vendors (SLAs and other contracts),
- software licenses,
- system users manuals,
- security manuals, and
- operating procedures.

The DR Coordinator should record plan modifications using a Version Control Maintenance Form, which lists the Serial number, Description of Change, Date of Change, Name & Signature of the person by whom it is reviewed, Name & Signature of the person by whom it is approved and the Date of Issue. Strict version control must be maintained by requesting old plans or plan pages to be returned to the DR Coordinator in exchange for the new plan or plan pages.
The DR Coordinator should also review following supporting information to ensure that the information is current and continues to meet system requirements adequately:

- Alternate site contract, including testing times
- Off-site storage contract
- Software licenses
- MOU or vendor SLA
- Hardware and software requirements
- System interconnection agreements

- Security requirements
- Recovery strategy
- Contingency policies
- Training and awareness materials
- Testing scope.

Although some changes may be quite visible, others will require additional analysis.
The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities.
A structured and controlled DR updating process will involve the use of formalized change control procedures under the control of the DR Team Head.

Key Personnel

Personnel Continuity Matrix

Sr. No.	Primary Role	Supporting Personnel	
		Administrative	*Operational*
1	Sr. VP – Ops	Head - IT, Head – Compliance	Head – IT, Head – Compliance
2	Head –IT	Sr. VP – Ops	Systems Engineer
3	Head –Compliance	Sr. VP – Ops	Head – IT, Head – Administration, Systems Engineer
4	Head – Administration	Sr. VP – Ops	Manager – Administration
5	Manager – Administration	Head – Administration	Head – Administration
6	Systems Engineer	Head – IT	Head – IT, Head – Compliance.

List of Process Specific Contacts and their backups

Description	Primary	Phone No	Escalation Backup	Phone No
BCP Coordinator	Vijay Tangri	+91 98992999936	Aman Chowdhury	+91 9899901134
Technical Operations Lead	Bijit Borah	+91 9350559120	L. Sridhar	+91 9899029366
Facilities Lead	Surinder Chaudhary	+91 9810272556	Anil Chauhan	+91 124 401 9657
IT Helpdesk	IT Helpdesk	+91 124 416 0510	Bijit Borah	+91 9350559120

Technical Escalation Matrix

IT Helpdesk	IT Helpdesk	helpdesk@copalpartners.com	Desk: +91 124 416 0510
Technical Lead	Bijit Borah, Head of Technical Operations	bijit_borah@copalpartners.com	Desk: +91 124 416 0578 Mobile: +91 9350559120
Operations Head	Erik Simonsen SVP, Operations	erik_simonsen@copalpartners.com	Desk: +91 124 416 0500 Mobile: +91 98182 11636
Country Head	Aman Chowdhury	aman_chowdhury@copalpartners.com	Desk: +91 124 416 0500 Mobile: +91 9899901134

APPENDIX F:

CONFIDENTIAL

Compliance Manual

Last Updated: June 2006

Table of Contents

Compliance Requirements

You are required to comply with the terms of this manual ("the Compliance Manual"), as amended from time to time. You are required on commencement of employment to sign a personal declaration acknowledging receipt of the manual and undertaking to observe both the spirit and the letter of its principles, procedures, rules and regulations in their entirety.

This Compliance Manual covers, inter alia, legal requirements regarding Insider Dealing and Market Abuse. It also sets out the Company's restrictions on personal dealings in securities. You are advised that the restrictions on personal dealings apply both to the employees and their closely connected persons as defined in this Compliance Manual. Any breach of either the letter or spirit may well result in disciplinary action being taken, which could result in your dismissal. The relevant Compliance Officer should always be consulted directly if you are in any doubt as to your responsibilities in this area. If you are not sure who to consult in this capacity ask your manager.

In order to protect the Company from unwarranted risk, you must immediately notify Human Resources of any material changes, either personal or financial, to your circumstances which may affect your ability to carry out your duties in a proper and professional manner. You must inform Human Resources of any changes to the personal information given on employment, any Court proceedings or judgments, bankruptcy proceedings, deeds of arrangement with creditors, conviction for criminal offences (excluding minor traffic offences but including dangerous or drunken driving), or similar matters in your place of employment or elsewhere. If you are in any doubt as to whether an event is noteworthy, you should consult your Compliance Officer or Human Resources at once. You accept that the Company, as a financial research institution, must be able to process information about criminal offences and criminal convictions for the purpose of preventing and detecting fraud and other offences and you consent to the lawful processing of any data referred to in this section 3.

You must notify the Human Resources department of any domestic, personal or business relationship with another employee. Each situation will be reviewed on an individual basis taking into consideration the risk posed to the business and its employees both now and in the future. Possible courses of action could include the redeployment of one or both parties to an alternative role with diminished risk or, in extreme circumstances, either party may be required to leave the Company.

During your employment including during any period of paid leave whether on notice of termination or otherwise you shall not, without the prior written consent of the Company, directly or indirectly be engaged, concerned, or interested in any capacity in any business, trade or occupation other than that of the Company. This includes but is not limited to the following applications:

- You may not hold more than 1% of the issued shares or securities of any companies which are listed or dealt with on any recognised stock exchange or market.

- You may not take up any other paid or unpaid employment whilst employed by the Company, whether on notice of termination or otherwise without the prior written consent of a Human Resources Director.

- If on joining the Company you already hold or subsequently you wish to take up any directorship, consultancy or other similar position in outside companies you must have the written approval of a Human Resources Director and the Head of Business. Where such appointments are approved, you will normally be required to account to the Company for the fees received or for benefits received in another form, e.g. stock or stock options. Approval is not necessary in respect of purely private arrangements (e.g. residents associations, golf clubs), but if you are in doubt please raise the issue with Human Resources.

Insider Dealing

Insider dealing is a criminal offence, prohibited under various Acts.

It happens when you use, or encourage others to use, information about a company which is not generally available (that you have got through inside knowledge or contacts), to deal for your own profit. It is irrelevant how the individual has come by the inside information. If known, all dealing is prohibited.

- **Dealings** – Relates to securities and in relation to such means not only acquiring or disposing of or subscribing or underwriting for securities but also includes inducing or attempting to induce any other person to do so or making or offering to make an agreement in relation to such.
- **Securities** – The term securities includes not only shares but also debentures (essentially any debt instrument of the company) and applies to these securities which have a dealing facility on a recognised stock exchange. The definition includes any right, option or obligation in respect of such securities. The law applies to transactions on the Stock Exchange and to off- market trading.

You are required on commencement of employment to provide the Company a detail list of all Securities (as defined above) you currently own, including but not limited to: number of securities, date of purchase, percentage ownership; and submit an official copy of your latest quarterly summary security report provided by all your brokerage firms

You must obtain clearance and written authorization from the Human Resources Manager to sell, acquire, or transfer any Security.

For a period of six months after termination of employment you will be prohibited to deal in any securities that due to having been connected with the Company you are in possession of information that is not generally available.

Indian Nationals are subject to legal restrictions on the ownership of foreign securities. For more information, contact the Human Resources Manager.

If you have knowledge of someone engaging in insider dealing you should contact the Human Resources Manager.

Engaging in Insider dealing is not only a breach to the confidentiality agreement between you and the Company but it will also result in an official criminal investigation and employment termination.

Market Abuse

The Code of Market Conduct deals with three broad types of behaviour that amount to market abuse.

- **Misuse of information** – behaviour based on information which is not generally available but which would be relevant to an investor's dealings in a particular investment and which is normally disclosed to the market.
- **Creating a false or misleading impression** – behaviour likely to give a false or misleading impression as to the supply or demand, price or value of an investment.
- **Distorting the market** – behaviour which interferes with the noral process of supply and demand and therefore manipulates the market price of an investment.

Even if you do not commit the abuse yourself, but instead require or encourage others to do so you are still incurring in Market Abuse.

Engaging in market abuse is not only a breach to the confidentiality agreement between you and the Company but it will also result in an official criminal investigation and employment termination.

Confidentiality

You acknowledge that during the ordinary course of your employment by the Company you may be exposed to information about the Company's business and that of its clients which amounts to a trade secret, which is confidential or is commercially sensitive and which may not be readily available to others engaged in similar business to that of the Company or to the general public ("Confidential Information"). You further acknowledge that if such information is disclosed to third parties it may cause harm to the Company's business.

You agree that you shall keep confidential and shall not at any time either during your employment or after its termination, for whatever reason, use, communicate or reveal to any person any Confidential Information concerning the business, finances, organisation or operation of the Company, its systems, techniques or know how or its clients which shall have come to your knowledge during the course of your employment, whether or not such information is reduced to tangible form or marked in writing as "confidential".

In the case it is needed; you may be required to sign additional Confidentiality agreements. These may be issued by Copal Research India Pvt. Ltd, Copal Partners Ltd or a client company.

You must maintain as confidential any and all information that you become aware of or that is in your keeping pertaining to the Company, the Company's clients, prospective clients, and former clients. Information includes all documents, electronic files, and oral information.

You shall take steps to ensure that you know to whom you are divulging information in the course of business and check what information it is relevant to give them.

The restrictions contained in this section shall not apply to:

- any disclosure or use authorised in advance in writing by the Company

  or required in the ordinary and proper course of your employment;
- any disclosure or use required by a Court or Tribunal of competent jurisdiction or as required by any appropriate regulatory authority;
- any information which you can demonstrate was known to you prior to the commencement of your employment by the Company;
- any information which is in the public domain otherwise than as a result of a breach of this section;
- information which consists solely of general know-how or general technique or of your general skill and knowledge; or
- any disclosure to the Compliance Department of the Company

where you have reasonable suspicions that a colleague is not observing the rules and procedures of the Compliance Manual;

You agree that any documents or other tangible materials supplied to or acquired by you which embody Confidential Information in whole or in part shall remain the property of the Company and you have no right, title or interest in such materials.

You will use all reasonable care to prevent the loss or inadvertent disclosure of information that is in your keeping. You will safeguard the integrity of physical documents, maintain the security of electronic documents through use of passwords, safeguard computers and laptops that contain confidential information, and use diligence when transmitting information via e-mail.

Upon request of the Company or its clients, you will return to the Company or the client any and all information in your keeping without retaining a copy.

You will take reasonable precautions when discarding information (including drafts of documents) that are consistent with maintaining confidentiality.

You will promptly notify the Company's officers of any loss or inadvertent disclosure of information to enable appropriate action to be taken that will minimize the consequences of the disclosure.

You shall not without the written permission of a duly authorised Director of the Company communicate directly or indirectly in any manner with the media or any agent of the media about the business, organisation or finance of the Company or its systems, techniques, know how or clients. For the purposes of this section "media" shall include television (terrestrial, satellite cable and digital), radio, newspapers and any other journalistic publications (whether in printed or electronic form).

Employees must not store confidential Company information on home computer equipment.

Personal Declaration

I, _____, have received and carefully read and reviewed

Copal Partners Ltd / Copal Research India Pvt. Limited ("the Company") Compliance Manual and

Company Employee Handbook ("Agreements"). The Company thoroughly and clearly has answered

all questions and doubts relating the terms and conditions expressed in these Agreements, and thus

I clearly understand and grasp the full extent of the Company's principles, procedures, rules and regulations.

I will undertake to observe both the spirit and the letter of the Agreements and understand that the provisions of this Agreement shall survive any termination of my employment or any termination of the Company's contractual agreements with its clients.

I have disclosed to the Company officials whether or not I owned any Securities (as defined in the Company's Compliance Agreement), and disclosed the required and pertinent official documentation.

I further understand that violation of the terms of this Agreement may constitute grounds for immediate termination of my employment with Copal Partners Ltd / Copal Research India Pvt. Limited.

Name:

_____ Date:

_____

Signature:

_____

Witn

ess: Name:

_____

Date: _____

Signature:

_____

Copal Partners

Securities Trading Authorization Request

I, _____, request Copal Partners Ltd / Copal Research India
Pvt. Limited ("the Company") authorization to: (check all that apply)

( ) Acquire Securities (as defined in the Company's Compliance Agreement) detail of which is described in the table below

Type of Security	Company	Ticker	Number of Securities	Will you own more than 1% of Company? (Yes/No) (in Affirmative case state exact percentage)

( ) Sell Securities (as defined in the Company's Compliance Agreement) detail of which is described
in the table below

Type of Security	Company	Ticker	Number of Securities	Did you own more than 1% of Company? (Yes/No) (in Affirmative case state exact percentage

( ) Transfer Securities (as defined in the Company's Compliance Agreement) detail of which is
described in the table below

Type of Security	Company	Ticker	Number of Securities	To Whom Will You Transfer the Securities to	What is that Person's or institution's Relationship to you

I understand that the Company can at its discretion not authorize (either totally or partially) this
request. I will be obliged to refrain from engaging in any unauthorized transactions.

Name: _____

Date: _____

Signature: _____