White Paper

Regulatory Compliance & Business Continuity Planning

June 15th, 2004

Insight Into Management & Technology Topics

iQknowledge

Prepared by:

InQuest Corporation

Table of Contents

EXECUTIVE SUMMARY 3
REGULATORY COMPLIANCE & BUSINESS CONTINUITY PLANNING 3
REGULATORY COMPLIANCE & BUSINESS CONTINUITY PLANNING 4
CORPORATE GOVERNANCE 4
COMPLIANCE FACTORS DRIVING IT SPENDING 6
REGULATORY ISSUES DRIVING DATA STORAGE REQUIREMENTS 7
COMPLIANCE AND CONTINUITY 7
CONCLUSION 9
APPENDIX A 10
Laws – Regulations & Technologies To Consider 10
InQuest's Compliance & Continuity Solutions 11

Executive Summary

One of the most forceful trends shaping both private and public organizations is the need to ensure that their information systems are accurate and compliant with regulatory mandates. Ensuring compliance with laws and regulations is a pressing demand for IT departments, and now IT must also be compliant with internal governance and operational requirements, incorporate best practices into their operations, and be cognizant of the requirements demanded by customers, partners, and employees. All of these initiatives may be considered a waste if IT fails to implement a culture of management compliance and satisfy the requirements of regulatory mandates to capture, retain and manage the corporations information in an effective and trustworthy manner.

A compelling reason to focus your organization on compliance and make it a strategic initiative is to reduce the cost of meeting individual regulations. The price tag for a single compliance initiative, Sarbanes-Oxley, drives home the point. In a January 2004 survey of 321 companies, industry group Financial Executives International found that for large companies, the average cost of compliance with Section 404—Management Assessment of Internal Controls — was $4.6 million, including 35,000 hours of internal staff time, $1.3 million for consulting and software and $1.5 million in new audit fees.

InQuest Corporation has identified at least eight Regulatory Compliance areas that have applicability to BCP –

1. **Data Retention & Storage**
2. **Information Lifecycle Management**
3. **Process Automation**
4. **Exception Handling**
5. **Risk, Security, Confidentiality & Privacy Management**
6. **Auditability & Traceability**
7. **Ability to Adapt to Changes in Regulation with a Change Management program**
8. **Reduction of Fraud & Error**

A compliance strategy provides a competitive edge. If your organization can respond quickly to new regulations while others in your industry remain stuck in 'tiger-team' mode, the advantage goes to you and your organization. The ability to respond to compliance requirements, in any operating situation, will differentiate you from your competitors in the eyes of your customers, employees, shareholders, and partners.

Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), Graham-Leach-Bliley (GLB)[1], and other industry-specific rule changes have ushered in a regulatory era that greatly values risk management and increases the penalties for companies and individuals whose risk-management practices are less than robust. Disaster recovery and business continuity represent a central component of a company's overarching risk-management strategy.

Companies that elevate business continuity and disaster recovery to a strategic level in their business and compliance activities do more than avoid risk. Stringent security and business-continuity standards focus improvements in performance and help to expand IT's capability to support the business. In addition, technologies and procedures that address security and continuity issues improve business processes and productivity, and help to mitigate costs associated with meeting compliance driven technology changes.

[1] See Appendix A: Laws – Regulations & Technology To Consider

Regulatory Compliance & Business Continuity Planning

61% of CIOs say they plan to increase IT spending to meet regulatory requirements.

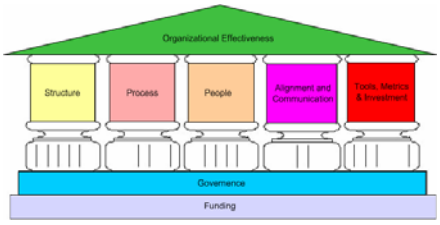
- CIO Insight, Feb 2004

The plethora of regulatory compliance rules that companies must be aware of and mitigate the risk of non-compliance is exhausting. The regulatory landscape is full of compliance land mines for the unaware organization. From Sarbanes-Oxley, HIPAA, Basel II, Graham-Leach-Bliley, SEC Rules 6835 & 17-a, TREAD Act, FCC-LSOG, USA Patriot Act, California Security Breach Notice Law and the list may as well go on ad infinitum. How do you make sense of the compliance issues, how do you monitor changes in the regulations, and where will the budget to support these initiatives come from? Bringing the introduction back to this papers topic: where is the integration point between regulatory compliance and business continuity planning? *Let's see if some light can be shed on this topic while using Sarbanes-Oxley compliance mandates as the measuring stick for requirements.*

"Today corporations are struggling to deal with a complex regulatory environment whose mandates have no budget allocations, while still managing tight IT budgets," is an interesting quote from Rich Mogull, research director for Gartner. On top of this problem, there is a maze of other IT-related challenges. Challenges that include, automating processes that are currently manual, multiple sources for information and data, the need to understand data and information lifecycles, and process and information auditability. Corporations struggle to keep their eyes on the regulatory strategic ball while they are juggling many tactical operational balls.

In many organizations, the first reaction to a new regulation is to create a 'tiger team' to address the issue. However, if you have these teams for three or more regulations, the redundancy makes no sense and just as importantly if the team is working in a vacuum and fails to include the business continuity teams you have lost the opportunity of economies of scale, a team with broad internal knowledge and a reduction of replicated efforts.

Corporate Governance



Gartner's Organizational Effectiveness Model

According to Gartner, five pillars support an organization's ability to prove operational effectiveness. The five pillars are:

1. STRUCTURE
2. PEOPLE & CULTURE
3. PROCESS
4. ALIGNMENT & COMMUNICATION
5. TOOLS, METRICS & INVESTMENT

These five pillars are supported by a foundation of FUNDING and GOVERNANCE. Corporate Governance has many components,

but one of its watchdog components is regulatory compliance. Regulatory compliance is one of the catalysts motivating organizations to do something serious about how they manage their business processes for both financial and IT objectives. Regulatory compliance is one of the biggest external influencers of today's corporate IT budget. Significant investment must be made to comply with provisions and this draws deep-interest in IT upgrade planning, budgeting, balanced-scorecard reporting, and analytic software as a means to improve performance and compliance. Compliance also has significant financial urgency for companies, as regulatory deadlines are everywhere. For example, compliance deadlines are staring healthcare professionals in the face. Beginning July 1st, 2004 the government began delaying payment to healthcare providers who treat Medicare patients and fail to submit electronic claims using a standard HIPAA reporting format. Publicly traded companies regulated by the SEC are struggling to meet the November 15th, 2004 deadline to comply with Sarbanes-Oxley. Can this renewed focus on corporate governance become the catalyst for establishing new levels of operational resilience and therefore drive focus to organizational business continuity planning?

Compliance initiatives, such as SOX, can be effectively implemented & leveraged if included in an organization's Business Continuity plan. Understanding the integration between business process and IT function is crucial to success.

- METAGroup 2003

For both commercial enterprises and government entities there are now strict rules establishing requirements for increased maturity in governance efforts in comparison to the rules that were in effect in the 1990's. Much of the new compliance initiatives are a direct result of the financial debacles experienced by Enron, WorldCom and others, as well as September 11th, 2001.

Regulatory compliance, in most cases, requires implementation of some kind of internal control and audit trail. A perfect example is Sarbanes-Oxley whose November 2004 deadline for Section 404 is fast approaching. Companies whose valuations are greater than $75 million must be able to prove that their internal controls and audit trails are capable of producing correct and certifiable data. This drives focus ensuring reporting capabilities are not impacted by a disaster of any magnitude in order to mitigate the risk of financial penalties. Companies must seek to ensure that compliance initiatives are supported by new technology and process investments as well as robust continuity of operations initiatives to satisfy regulatory mandates. Even if things are running smoothly in your IT organization, it is likely that you may be wondering what would happen in the event of a real-life disaster to your organization. In other words, if the lights go out, will you really be able to meet your regulatory compliance mandates?

It may be tempting to think of this as just a Sarbanes-Oxley or HIPAA problem, but it really is part of a long-term trend toward defining what corporate accountability means in a digital information era. Organizations will need to look beyond their current practices and adopt a broad and resilient framework for regulatory compliance that is capable of addressing current and

future needs during normal and emergency operations. Compliance is required in almost all aspects of business – a critical challenge in achieving and maintaining compliance will be to ensure not only that all those responsible within the company are able to avoid infringing the regulations – but also that concrete evidence is available to demonstrate process and data integrity.

Compliance Factors Driving IT Spending

Sarbanes-Oxley:

- **Section 802 –** *Ensure authentic, immutable records and retention.*
- **Section 409 –** *Disclose to the public on a "rapid and current basis" material changes to the firm's financial condition.*
- **Section 302 –** *Officers of the company must make representations related to the controls, procedures, internal controls, and assurance from fraud.*
- **Section 404 –** *Provide an annual assessment as to the effectiveness of internal controls in financial reporting, and obtain an attestation from external auditors that the controls are effective.*

Given regulatory compliance, according to InfoWorld, it is no surprise that regulatory mandates rank high amongst those "Factors Driving 2004 IT Spending." In a survey of 618 respondents' lists of priorities, improving data protection and disaster recovery plans took top billing followed closely by data archiving and email. These are all extremely important components of the regulatory mandates on most company's front burner issues.

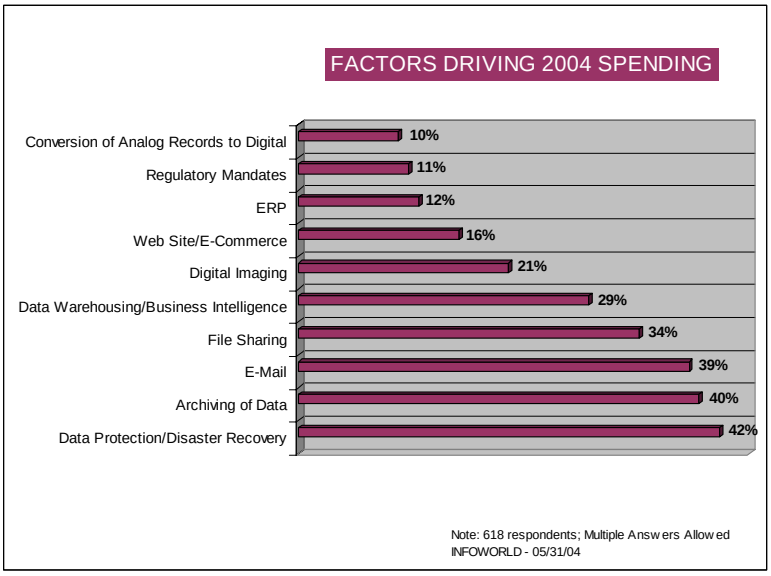


Figure 1 - Factors Driving 2004 IT Spending

The demands of regulatory mandates, data protection, and disaster recovery have resulted in a great deal of new IT-related spending. Many industry analysts estimate that roughly half of all enterprises will need to implement new systems for record and e-mail management. Companies will have to rethink how they store, access, retrieve, and recover data. In addition, we must not forget the speed with which data must be retrieved and recovered. This requirement, outlined in Section 409 of Sarbanes-Oxley, speaks to deadlines for compliance; and if you do not believe this is an important issue think back to March 2004 when the SEC fined Bank of America approximately $10 million because it was unable to respond to an information disclosure request in a *reasonable* amount of time.

Regulatory Issues Driving Data Storage Requirements

Section 404 of Sarbanes-Oxley requires compliance audit trails not just for financial records but also, e-mail, voice-mail, and video records. The issue of new data types is becoming a management headache for corporations because of their storage requirements. Other IT processes affected by Section 404 include security administration, application-change control, data management and disaster recovery, data center operations and asset management.

While Sarbanes-Oxley is financial legislation, at its heart it is about ensuring that internal controls or rules are in place to govern the creation and documentation of information in financial settlements. Since its systems are used to generate, change, house and transport that data, CIOs have to build the controls that ensure the information stands up to audit scrutiny.

- CIO Magazine, May 2003

The implications for data storage, access, retrieval, and recovery for all compliance records become impressive. It is estimated, by AMR Research, that storage requirements for *all* compliance records will grow from 300 petabytes per year to 1.6 exabytes per year by 2006. So, with all this stored data, it is assumed that each record will comply with the definition of being trustworthy.

To be trustworthy data must meet five key qualities:

1. *Integrity* – the ability to demonstrate its content has not been changed
2. *Accuracy* – contains the information it is suppose to contain over its entire lifespan
3. *Authenticity* – the source of the content and who had control over it can be demonstrated
4. *Accessibility* – the record can be accessed in a timely fashion and is not threatened by poor indexing, the lifespan of the storage media, hardware obsolescence, software incompatibility and environmental degradation
5. *Confidentiality* – the ability to demonstrate the content is only accessible by those who need to view and mange it

All five qualities point to the need for corporations to ensure their business continuity house is in order and capable of ensuring data integrity, accuracy, authenticity and accessibility under any circumstance.

IT will play a key role in these compliance initiatives. The question is, will the role be one of leadership or mere execution? Can IT create systems and processes that allow the corporation to comply easily with any new regulation it encounters, regardless of that regulation's specifics, breadth of mandate and origin? These are key questions, and millions of dollars ride on the answers from an investment and regulatory penalty perspective.

Compliance and Continuity

It is easy to demonstrate a straight-line relationship with the key data characteristics identified above, regulatory mandates and the need for business continuity planning to ensure trustworthiness. Compliance initiatives should be integrated with business

continuity efforts to gain efficiencies of scale and minimize corporate risk exposure.

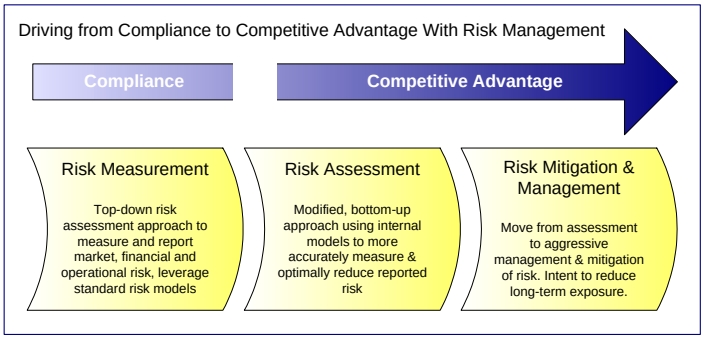


Figure 2 – Risk Management – Compliance to Competitive Advantage

The similarities between regulatory compliance efforts and a business continuity effort should not be ignored. When executed with a best practice framework, a comprehensive business impact analysis (BIA) and risk assessment, both core components of business continuity planning, will help to identify risk and control deficiencies that can result in process and system downtime. A BIA includes data gathering, process mapping and risk identification, and all core requirements of Section 404 of Sarbanes-Oxley. Conversely, a thorough Sarbanes-Oxley compliance effort should yield valuable information for developing or updating a business continuity plan. Significant value may be derived by sharing the detailed analyses of BCP and Sarbanes-Oxley efforts between the groups involved in the implementations. A best practice would suggest these initiatives incorporate cross-boundary teams involved in both efforts to ensure cross-pollination of findings.

A CIO Insight and Gartner research study asked 600 executives and managers responsible for compliance initiatives in their companies what they believed was the greatest obstacle to overcome to become Sarbanes-Oxley compliant. Approximately thirty-six and a half percent of respondents were concerned about insuring adequate security and business continuity programs to support compliance initiatives. Oddly, nearly one-fifth of the respondents were also concerned of a lack of cooperation between IT and business units; this is believed to be a major obstacle to gaining real business value from regulatory compliance initiatives.

Conclusion

Regulatory mandates allow the modern organization to rely on electronic records and information for more purposes than ever before. This in-turn creates a new directive for IT organizations to store, access, retrieve, and recover business information in an efficient, secure, and trustworthy manner. Statutes such as Sarbanes-Oxley and regulations like SEC Rule 17a-4, and court rules require records and evidence to be complete, reliable, accurate, and to have integrity. The cost to organizations who fail to meet these requirements can be overwhelming.

Technology will play a critical role in a company's ability to comply with new financial reporting rules, but only after making sure internal processes and controls are in order.

IT departments responsible for ensuring corporate compliance have never been more important. IT personnel must ensure that the information stored within information systems can be relied upon for an ever-increasing range of legal and regulatory purposes. This mandate is overwhelming evidence that as organizations pursue regulatory compliance initiatives they must:

1. Acknowledge the need and interrelation of business continuity plans
2. Modify implemented plans to accommodate regulatory needs
3. Maintain their plans with an eye towards the ever-changing regulatory landscape.

Business continuity is much more than an IT issue, it's a business issue and the model has changed. A company's executive team now faces legal responsibility for upholding fiscal and fiduciary obligations. By building a solid infrastructure and compliance-focused culture that supports the business effectively; companies can realize a solid ROI with regulatory compliance investments. The ability to respond to compliance requirements in any operational or emergency situation will differentiate your organization from your competitors in the eyes of your customers, employees, shareholders, and partners.

Appendix A

Laws – Regulations & Technologies To Consider

Laws & Regulations	Who Should Be Concerned	Key Provisions	IT/Risk Management Impact
Sarbanes-Oxley (SOX)	Public Companies Filing in the USA	▪ Requires companies to take great care that their financial reporting is accurate, and stipulates tough criminal penalties for non-compliance ▪ Section 404 requires companies to perform a self-assessment of business process risks	▪ Greater IT responsibility for the data in their systems, not just for the systems themselves ▪ Greater visibility of compliance, records management, and IT governance issues at the exxecutive level
Health Insurance Poratbility & Accountability Act (HIPAA)	Healthcare Providers, Healthcare Insurers, All organizations handling healthcare information	Three Technology and One Administrative Categories: ▪ Transactions Standards & Code Sets ▪ National Identifiers ▪ Security ▪ Privacy	▪ Greater IT responsibility for the data in their systems, not just for the systems themselves ▪ Greater visibility of compliance, records management, and IT governance issues at the exxecutive level
17 CFR 240.17a-4 (SEC Rule 17a-4)	SEC-regulated Companies	▪ Allows companies to store records in electronic form	▪ Storage systems must have "non-rewritable-non-erasable" functionality and meet several additional functional requirements
21 CFR Part 11	FDA-regulated companies	▪ Allows companies to store records in electronic form and use electronic signatures	▪ Mandates several detailed functional and securtity requirements for systems used to manage regulated records
IRS Revenue Procedure Ruling 97-22	All organizations subject to IRS regulations	▪ Allows organizations to maintain required records in electronic form	▪ Several requirements for electronic storage systems are stipulated, including "controls to ensure the integrity, accuracy, and reliability" of the system ▪ IT departments must ensure that e-record storage systems are compliant with these requirem
Governent Paper Work Elimination Act (GPEA)	Government Agencies	▪ Provides general legal equivalence between e-records / e-signatures and their paper counterparts in federal government activities ▪ Requires some agencies to adopt electronic processes	▪ Encouraged many regulators to adopt rules allowing companies to file and retain required documents in electronic form; however many regulatorsrequire specific forms and controls

Technologies Involved in Compliance								
Source: IDC, 2004	**SOX**	**HIPAA**	**GLB**	**SEC 17A-4**	**21 CFR Part 2**	**Basel II**	**USA Patriot Act**	**Calif. SB 1386**
Financial Compliance	✓					✓		
ERP	✓					✓		
Business Intelligence & Data Warehousing	✓					✓		
Content / Document Management & Search	✓	✓	✓	✓	✓	✓	✓	✓
Data / Application Integration	✓				✓	✓		
Business Process Automation	✓	✓			✓	✓		
Records Management & Archiving	✓	✓		✓		✓	✓	
Storage	✓	✓		✓	✓	✓	✓	
Security	✓	✓	✓	✓	✓	✓	✓	✓

SOX – Sarbanes Oxley
HIPAA – Health Insurance Portability & Accountability Act
GLB – Graham Leach Bliley

InQuest's Compliance & Continuity Solutions

Are you still struggling with how to address regulatory compliance mandates? InQuest's Compliance & Business Continuity solutions may be your answer. With compliance deadlines and sporadic regulatory audits becoming the norm, establishing the proper safeguards to protect your proprietary information is more challenging than ever. Adding to the challenge is the lack of a common language among regulators, standards organizations, consumers, and developers. Plus, there is a lack of a common structure for expressing requirements and assurance, and there is the need for credible organizations to evaluate requirements and validate compliance. You may need assistance translating the interpretation of regulations to identifying the proper technology and control measures to support your compliance program. We have the experienced personnel to support you in developing, deploying, and monitoring all your compliance initiatives.

InQuest removes the challenges of compliance and business continuity with our Business Continuity Management Framework. Using InQuest's seven-phase approach to compliance and four-phase approach to business continuity we ensure effective practices are used to springboard your compliance and continuity initiatives to a successful conclusion.

InQuest's experience and certified consultants, tools and intellectual property allows us to quickly assess, develop, implement, and test compliance and continuity initiatives for your organization.

InQuest's Seven Phase Best Practices Framework for Achieving Regulatory Compliance:

1. Assessment
2. Goal Definition
3. Gap Analysis
4. Architecture Design
5. Implementation Plan Development
6. Plan Implementation
7. Ongoing Administration & Validation

InQuest Compliance Service Offerings:

- Regulatory Exposure Assessment
- Compliance Organization & Governance
- Compliance Policy Gap Analysis
- Regulatory Risk Assessment
- Third Party Risk Management
- Compliance Implementation Strategic Planning

InQuest's Four Phase Best Practices Framework for Achieving Operational Resilience Through Business Continuity:

1. Discovery & Analysis
2. Plan Development
3. Plan Implementation
4. Ongoing Administration & Validation

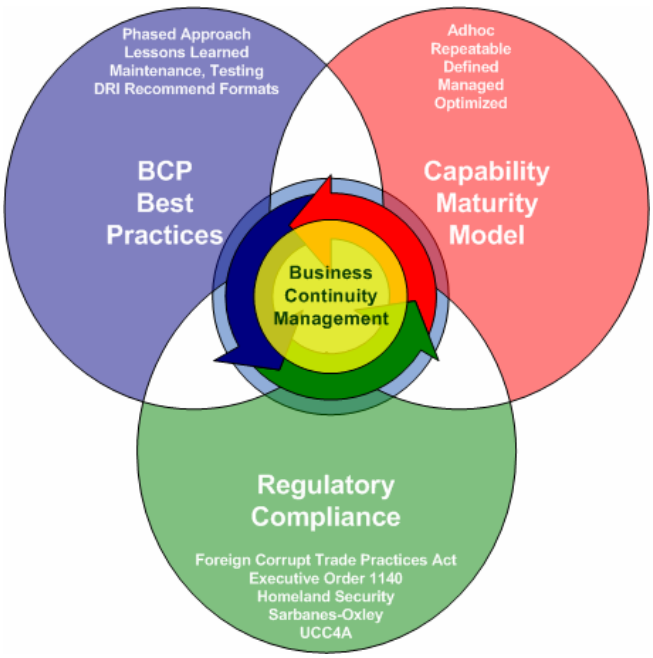
InQuest Business Continuity Service Offerings:

- Risk Assessment & Business Impact Analysis
- Recovery & Restoration Strategies
- Plan Development & Implementation
- Testing & Administration
- Plan Audit Services & Capability Assessment

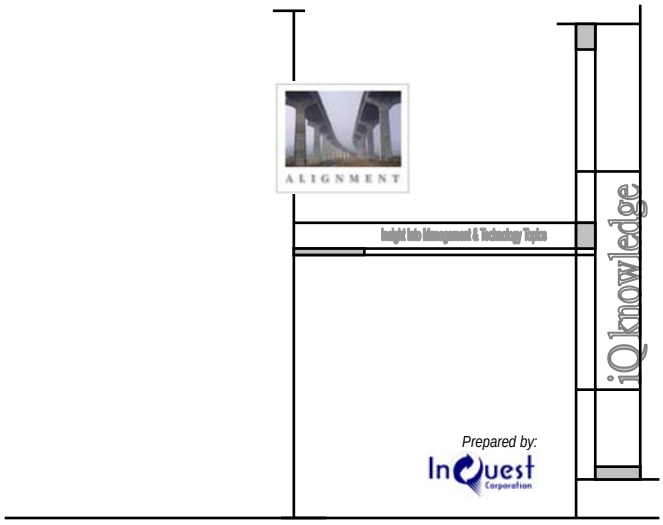
InQuest Corporation Differentiators:

- Highly-trained, certified, and experienced solutions consultants
- Customized Solutions with a methodical framework approach
- Extensive Industry Experience
- Access to experts in multiple IT disciplines
- Vendor Independence

InQuest Corporation collects and distills industry best practices in business continuity, security and other Information Technology areas. InQuest can deliver timely and effective enterprise security tailored to meet your organization's specific needs.



InQuest Corporation is pleased to present iQknowledge©, a series of whitepapers to assist organization's in making good management and technology decisions to support their business needs.



InQuest Corporation
3913 Newhall Drive
Plano, TX 75023
Tel: 214-289-4965
www.inquest-corp.com