

# FINsights

Technology Insights for the Financial Services Industry

Governance, Risk and Compliance »



Infosys®

POWERED BY INTELLECT  
DRIVEN BY VALUES.

# Contents

## From the Editors Desk

Strategic themes in Risk and Compliance .....	02
<i>Ashok Vemuri</i>	
Red light, green light – playing the risk game .....	06
<i>Adam D. Honore</i>	
Sub-prime crisis and credit risk measurement: lessons learnt.....	11
<i>Thadi Murali, Srividhya Muralikrishnan and Balaji Yellavalli</i>	
Credit risk management: back to basics .....	17
<i>Godwin George, Arup Sinha and Thadi Murali</i>	
Risk Measurement: It's all about data, data and master data.....	24
<i>Anita Stephen, Sabitha Vuppula and Abhijit Ghosh</i>	
Raising the bar: Executive risk reporting using fractal maps.....	29
<i>Raghu Anantharam and Shriram Subramanian</i>	
Navigating through the compliance maze in a post-merger world.....	33
<i>Debashis Pradhan and Naveen Balawat</i>	
Managing the problem within - Employee Surveillance.....	39
<i>Anand Bhushan, Debodeb Datta and Rajesh Menon</i>	
Addressing the partial compliance trap in the wealth management industry.....	45
<i>Bob Skea and Vikesh Gupta</i>	
Demystifying financial compliance through an integrated IT framework .....	50
<i>Ravishankar N and Ramachandran Sundaresan</i>	
Integrated Controls Management– a cost effective approach to implementing GRC..	55
<i>Uttam Purushottam, Satnam Gill and Ashwin Roongta</i>	
Conversations with Tim Leech – Perspectives from an industry expert.....	61
<i>Q &amp; A session conducted by Satnam Gill</i>	
Leveraging SaaS to manage GRC.....	66
<i>Ravi U. and Vishakha C.</i>	
Case study – Information Risk Management: A mandatory need .....	71
<i>Amar Bawagi and Viswananath Shenoy</i>	

## From the Editors Desk

We are delighted to present the second issue of the Infosys Banking and Capital Markets journal FINsights. The spotlight in this issue is on Governance, Risk and Compliance and the compilation of articles reflect perspectives on risk and its measurement, governance, the compliance conundrum and our take on the priorities in risk and compliance and their technology implications in the coming years.

The increased incidence of failures in the financial services marketplace over the past decade has given visibility to the science (and art) of understanding and measuring risk in running a business, making strategic and tactical decisions and participating in markets and economies that are increasingly linked in a flattening world. A recent such event, covered in one of the articles, has been the sub-prime crisis and the unforeseen ripple effects in markets in distant parts of the world.

As always we have tried to reflect in these articles the unique value that Infosys brings to its clients through a combination of deep domain understanding, technology best practices and global sourcing expertise. The article on sub-prime crisis reflects the current challenges in credit risk measurement and brings a perspective that combines credit risk measurement approaches with a global knowledge process outsourcing (KPO) option.

Risk and compliance is a multi faceted animal and the focus in the past few years has been on giving it a holistic view through a unified Governance, Risk and Compliance (GRC) program. The articles featured on GRC explore integrated controls to implement GRC, use of SaaS in GRC and industry perspectives on GRC and the road ahead. In the area of compliance, the articles look at addressing compliance challenges, an aspect of internal compliance namely employee surveillance and the partial compliance challenge in the wealth management industry. Our articles on risk address credit risk management, the role of master data in risk measurement and risk reporting. Included in this issue is also a case study highlighting the importance of Information Risk Management (IRM).

We would like to thank all the authors from Infosys as well as external contributors - Adam D. Honoré from Aite Group, Tim Leech from Navigant Consulting and Bob Skea of Northstar Systems. As always, we look forward to your queries or comments on Governance, Risk and Compliance or any feedback and suggestions in making FINsights a more relevant and topical journal.

Happy reading and all the best for the new year 2008!

**Balaji Yellavalli and Sudhir Singh**  
*Editors*

## FINsights Editorial Board

### **Balaji Yellavalli**

*Associate Vice President  
Banking & Capital Markets Group*

### **Edward L Smith**

*Associate Vice President  
Banking & Capital Markets Group*

### **Jonathan Stauber**

*Vice President  
Banking & Capital Markets Group*

### **Lars Skari**

*Practice Leader  
Infosys Consulting*

### **Thadi Murali**

*Senior Principal  
Banking & Capital Markets Group*

### **Mohit Joshi**

*Global Head of Sales  
Banking & Capital Markets Group*

### **Pankaj Kulkarni**

*Senior Engagement Manager  
Banking & Capital Markets Group*

### **Roopa Bhandarkar**

*Senior Engagement Manager  
Banking & Capital Markets Group*

### **Sudhir Singh**

*Associate Vice President  
Banking & Capital Markets Group*

# FINsights

Technology Insights for the Financial Services Industry



## Managing the problem within - Employee Surveillance

This article provides insights into challenges faced by the current employee surveillance programs and outlines an approach that could reduce companies exposure to the 'insider threat'.

Anand Bhushan  
Senior Associate  
Infosys Technologies Limited

Debodeb Datta  
Senior Associate  
Infosys Technologies Limited

Rajesh Menon  
Senior Principal  
Infosys Technologies Limited

## Introduction

Conflicts of interest and internal fraud are probably amongst the oldest and most pervasive principal-agent problems faced by a company, they cost companies an estimate of 3 to 5% of their revenue, apart from impacting their market reputation.

Significant advancements made in customer surveillance programs, in response to regulations such as the Patriot Act, over the past few years, have substantially reduced companies' exposure to external threats. However, programs designed to tackle internal threats have lacked the rigor, focus and budget support required to ensure their effectiveness. Increasingly complex product landscape, Governance policies and internal fraud sophistication have served as catalysts to further increase the costs and risks associated with insider threats.

Regulators are taking a closer look at this area, and there is the threat of increased regulation and higher penalties. Driven by the need to mitigate operational losses and reputation risks, firms are in need of an enhanced solution to tackle employee surveillance issues ranging from internal fraud to conflicts of interest.

### Employee Surveillance programs - Current State

Most companies have paper based, manual, inconsistent and non-structured programs. These approaches are probably enough for regulatory purposes but fail to meet their real objective – managing internal fraud.

### Flat world forces - A new set of challenges

Flat world forces are changing the financial services

industry landscape. Introduction of new and complex products and services, increased cross border transactions, improved flow of information across the globe while resulting in phenomenal business opportunities are creating a fresh set of challenges from the employee surveillance perspective.

### Increased sophistication of new products and services

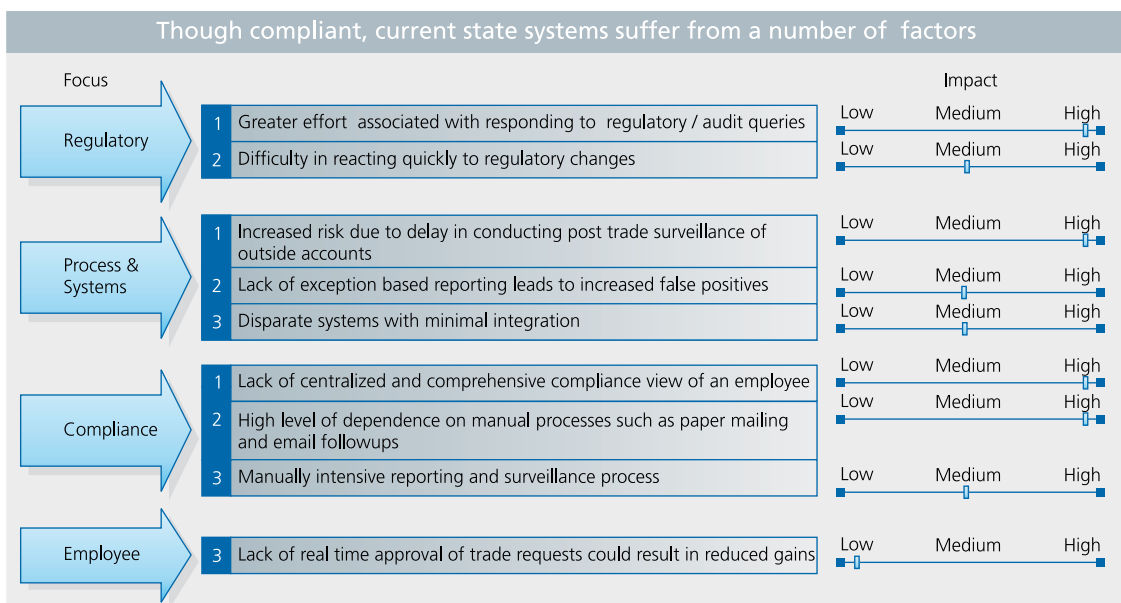
The increased complexity of new offerings has in turn created additional opportunities for internal fraud. Apart from needing sophisticated detection methods, the speed at which new products are introduced by institutions to ensure their market leadership/ dominance further impede the success of the detection efforts. The fraudster would have long moved on to the next product/ service by the time surveillance programs are in place for a given product.

### Increased organizational complexity

Talent everywhere! - The opening of emerging economies is providing greater access to skilled talent pools as well as new growing markets. As organizations grow, so do their complexities. The challenges of monitoring a global workforce are quite daunting. Business processes are getting complex, cultural issues are arising, inclusion of vendors or partners are enhancing surveillance concerns, not to forget the diversity of laws related to different geographical locations. There is an urgent need to move away from siloed approaches to enterprise wide surveillance programs.

### Increased data volume, free flow of information

Explosion in volumes of data combined with free flow of information is a true surveillance nightmare !!



Surveillance systems not only need to plough through volumes to detect the 'needle in the haystack', but also have the ability to detect parties acting in concert to provide investigators with the true picture of a potential fraud. Most surveillance processes are still handled manually, others which employ sophisticated systems generate so much noise/ false positives that the actual anomalies may go through undetected.

### Increased penalties by regulatory bodies

Laws are getting stringent and penalties levied on organizations are running into millions of dollars. There are a plethora of regulations that financial institutions operating in multiple markets need to deal with.

- In 2006, a large investment bank agreed to a \$10 million settlement with SEC primarily due to the company's failure to conduct trading surveillance on approximately 900 employees.
- Similarly in 2007, the NASD (National Association of Securities Dealers) fined a large asset manager \$3.75 million for failure to supervise certain individuals for compliance with the firm's "ethics and conflict of interest" policies.

Apart from fines paid, these incidents can do irreparable damage to the firms market reputation.

### Employee Surveillance programs - Key drivers

Annual Attestation & 407 Processing	Pre-trade clearance	Post-trade monitoring & surveillance
<ul style="list-style-type: none"> <li>▪ Create and leverage employee centric views</li> <li>▪ Manage annual and periodic attestation process</li> <li>▪ Incorporate ability to request and process exceptions</li> <li>▪ Support 407 processing (Paper based &amp; electronic)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Identify info sensitive employee</li> <li>▪ Manage restricted lists</li> <li>▪ Leverage rules based frameworks to detect exceptions</li> <li>▪ Achieve real time approval of trade requests</li> </ul>	<ul style="list-style-type: none"> <li>▪ Monitor employee trading in person and related accounts</li> <li>▪ Customize pre-built rules frameworks to detect activities of interest e.g front running, market timing</li> <li>▪ Leverage exception based reporting tools</li> </ul>

- **Access to information:** Controls defined around internal systems and applications that employees are authorized to access, internet access related controls and data security related controls fall under this category.
- **Exchange of information:** Controls defined to screen incoming and out going emails, chinese walls to ensure conflicts management belong to this category
- **Activity related surveillance:** Pre trade and Post trade compliance in employee accounts, monitoring gifts & contributions, control room and grey list surveillance are examples of activity related controls.

Activity related surveillance is the area where surveillance programs in most institutions are the most simplistic today and consequently need the maximum focus.

### Activity based employee surveillance platforms

Typically there are 3 facets to an activity based employee surveillance platform.

- **Collation of employee account related information** i.e details of brokerage and bank accounts held internally and with other firms. Based on the position held and level of sensitive information the employee has access to, these could include accounts of immediate family members. External firms provide periodic data about activity happening in these accounts.
- **Pre trade clearance:** Clearances requested by employees ahead of any trade they plan to execute. The approval process, decision criteria would be driven by the information access level of a given employee.
- **Post trade monitoring:** Use of behavior detection systems to identify possible violations which include front running, price manipulation, trading on restricted information etc.

An effective surveillance and monitoring program should adopt a rules based approach to surveillance and aim at increasing the straight through nature of most processes. Less manual intensive processes combined with reduction of false positives and creation of 360 degree views can dramatically improve the quality of surveillance and

productivity of the compliance organization.

There is a need to move away from siloed systems to an enterprise wide system with interfaces supporting informational needs required from internal and external sources e.g HR systems, Order Management systems, External brokerages/banks. Rules engines apply pre-specified rules on the reference and transactional information to create exceptions which can be prioritized using scoring algorithms.

Technologies such as workflow automation and case management can greatly enhance the efficiency of compliance employees. A workflow system can route a pre-clearance request to the appropriate managers for review and approval. The request once approved can be

routed to order management systems for trade execution. Case Management tools can automatically connect related data to assist in decision making.

- Focus on minimizing false positives: Instead of searching for the proverbial needle in haystack, an exception based surveillance system will allow

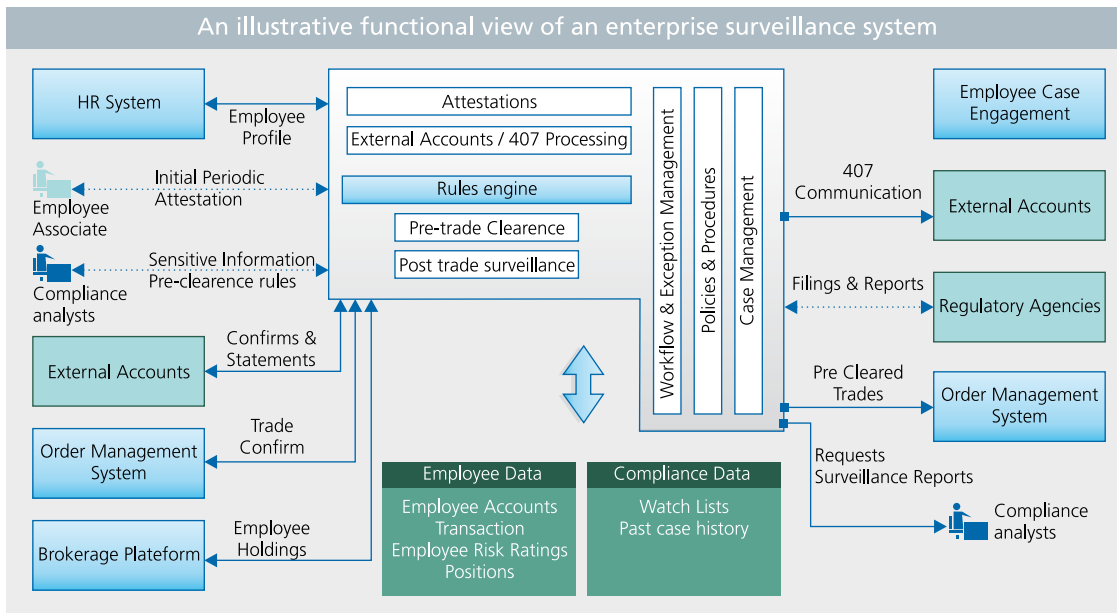


Fig 1: An illustrative functional view of an enterprise surveillance system

In addition to enhancing the quality of surveillance, enterprise wide approaches to surveillance have the following benefits:

- It enables a centralized and systematic approach to surveillance allowing for specialization of resources and promoting greater flexibility.
- It facilitates better and easier administration of corporate rules and policies.
- It allows for firms to consistently expand the scope of surveillance, facilitates quicker adoption of regulatory changes.

Based on our industry experience the following best practices can greatly improve the effectiveness of a surveillance program.

- When it comes to surveillance, everyone is not equal: It would seem intuitive that employees with greater access to information should be under greater scrutiny in comparison to an employee with limited access to material information. However, a number of firms find it very difficult to classify their employees in this manner. Investments in building a risk based classification of employees, contingent workers, consultants etc. can lead to significant improvements in conducting effective surveillance.

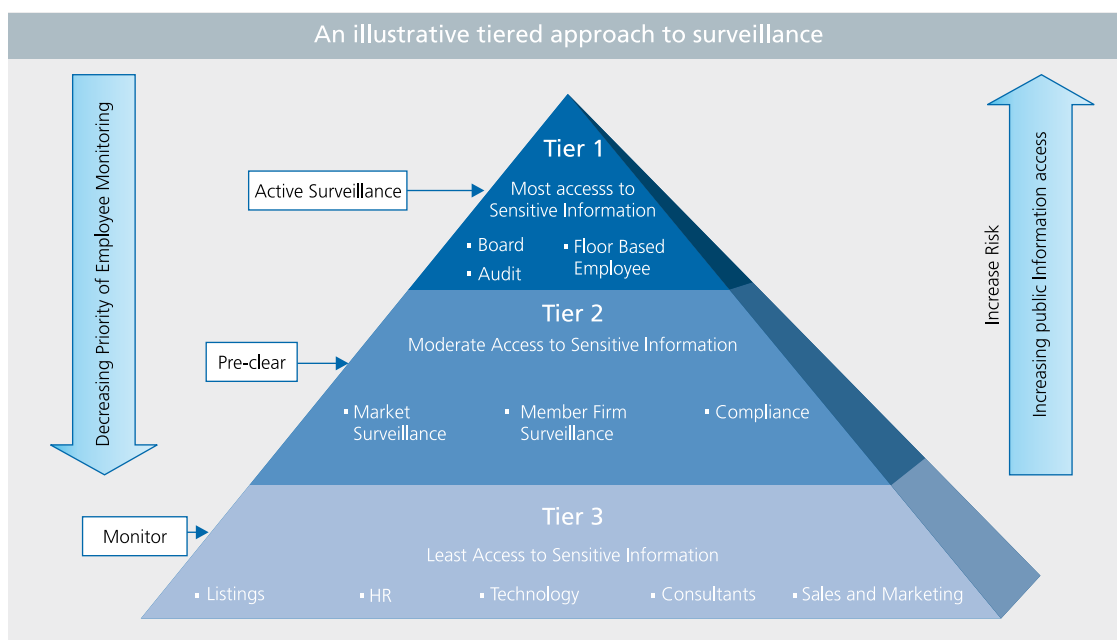
compliance resources to be focused more on solving the right case instead of finding the right case.

- Create unified views: Systems which are designed to provide a unified view of an employee across different types of surveillance related exception would be the most effective as they empower the analyst with the required information to efficiently investigate an exception. Detection of patterns, parties acting in concert are also best achieved in systems that support 360 degree views.
- Improve end user experience: This applies from the perspectives of both, the compliance analyst and employees who are being monitored. Case management tools, 360 degree views, rules based platform have led to dramatic improvements in the productivity of compliance teams, quality of surveillance. Further, efficiencies in the underlying compliance processes e.g improvements in turnaround times of pre trade compliance approvals have led to greater adoption of these systems by the employees.

## Changing regulatory landscape

Employee trading surveillance is no longer limited to select geographies/ regulators. There are a plethora of regulations that financial institutions operating in multiple markets need to deal with. These include,

- Ontario Securities Act Part XXI Investment Advisers Act Rule 204A-1 & Investment Company Act Rule 17j-1 in North America.



- European legislation include Financial Services and Markets Act (UK), Securities Trading Act (Germany), General regulations of the Autorite des Marches Financiers (France), Law on the Supervision of the Financial Sector and on Financial Services (Belgian market).
- In the Asia/Pacific region, Australia, Hong Kong, Singapore and India are among the countries that have defined comprehensive employee surveillance regulations.

Large financial conglomerates operating across multiple continents, while ensuring consistency in their employee surveillance policies are challenged by the variation in the local regulation relating to collection and usage of employee data. The European Union Privacy Directive, Japan's Law on the Protection of Personal Information and Australia's Privacy Act are some examples.

Markets in Financial Directives (MiFID), in Europe apart from ensuring best price discovery and execution

mechanism also focuses on preventing conflict of interest. With MiFID driving the investment management firms to rewrite/ update policies and approach to supervision and recordkeeping since it went into force from November, 2007, we will be seeing some major changes in the employee surveillance space in the months to come.

## Conclusion

In conclusion, we would like to reiterate that the key to an efficient employee surveillance program is adopting an enterprise wide platform supported by rules based approach, straight through processes and unified views coupled with ease of use. The platform should be flexible and scalable to meet the differing regulations across various markets and geographies. This is no small task and is best carried out by first defining a roadmap and then undertaking a series of small and coordinated projects with measurable benefits to attain this goal.



**Anand Bhushan**  
*Senior Associate*  
*Infosys Technologies Limited*

Anand is a Senior Associate with the Banking and Capital Markets practice of Infosys Consulting. He has over 8 years of consulting experience in a variety of projects to define technology strategy and operational improvements. His areas of expertise are in compliance, wealth and investment management.



**Debodeb Datta**  
*Senior Associate*  
*Infosys Technologies Limited*

Debodeb is an Associate with the Banking and Capital Markets practice of Infosys Consulting. He has more than 5 years of consulting experience in the financial services industry. His area of focus is compliance.



**Rajesh Menon**  
*Senior Principal*  
*Infosys Technologies Limited*

Rajesh is a Partner with the Banking and Capital Markets practice of Infosys Consulting. He has over 14 years of experience in the Financial Services industry and has been involved in advising several Wall Street firms in various aspects relating to their compliance programs and Operations. His areas of expertise are in compliance and investment banking.

For information on obtaining additional copies, reprinting or translating articles, and all other correspondence, please e-mail: [bcm@infosys.com](mailto:bcm@infosys.com).

## Global Presence

### North America

Atlanta, Bellevue, Bridgewater, Charlotte, Detroit, Fremont, Houston, Lake Forest, Lisle, Mexico, New York, Phoenix, Plano, Quincy, Reston, Toronto

### Europe

Brussels, Copenhagen, Frankfurt, Geneva, Helsinki, London, Milano, Oslo, Paris, Stockholm, Stuttgart, Utrecht, Zurich

### Asia Pacific

Beijing, Hong Kong, Mauritius, Melbourne, Shanghai, Sharjah, Sydney, Tokyo

### India

Bangalore, Bhubaneswar, Chandigarh, Chennai, Hyderabad, Mangalore, Mumbai, Mysore, New Delhi, Pune, Thiruvananthapuram

For more information, contact [bcm@infosys.com](mailto:bcm@infosys.com)

## About Infosys

Infosys Technologies Ltd. (NASDAQ: INFY) defines, designs and delivers IT-enabled business solutions that help Global 2000 companies win in a flat world. These solutions focus on providing strategic differentiation and operational superiority to clients. Infosys creates these solutions for its clients by leveraging its domain and business expertise along with a complete range of services. With Infosys, clients are assured of a transparent business partner, world-class processes, speed of execution and the power to stretch their IT budget by leveraging the Global Delivery Model that Infosys pioneered.

**Infosys**<sup>®</sup>  
POWERED BY INTELLECT  
DRIVEN BY VALUES

[www.infosys.com](http://www.infosys.com)