IBM

IBM Safety & Security

Security for the New Era

Urgent Regulatory Imperatives

New York RACF Users Group Meeting

Priscilla Rabb Ayres
Global Regulatory and Compliance
Solution Executive

Bob Kennedy, CFP, CISSP
National Solutions Executive
IBM Safety and Security

ON DEMAND BUSINESS™

April 27, 2005

Agenda

- Importance of security and how it relates to regulatory compliance
- Security environmental changes and trends (The Bad Guys Are Winning!)
- IBM's leadership in the security area
- Regulation in the Information Age: Background
  - What is new about regulation in the 21st century?
  - Drivers for change
  - The new regulatory paradigm: Risk-Based Supervision
- Where are we now?
- The critical role of data integrity and security in the new Regulatory regime
- IBM Software and Services for Sarbanes–Oxley, Patriot Act, GLB etc.
- Summary

Definitions (simplified)

- **Security – Confidentiality, Integrity and Availability of company Assets**
- **Privacy – Requires the Consent of the Data Owner**
- **Regulatory Compliance – Usually encompasses the Integrity or Confidentiality of the Data**

Source: NIST Pub 800-53

Security Controls:

- Administrative – Policies, standards, procedures, screening personnel, security awareness
- Technical – Logical access controls, encryption, security devices, identification and authorization
- Physical – Facility protection, guards, locks, monitoring, environmental controls, alarms

Risk Management:

- Identifying, assessing and reducing risk to an acceptable level
- Mitigate, transfer or accept

Threats and Current Events

- **Hackers penetrate global finance firms**
  - Deloitte's 2004 Global Security Survey, most multinational financial institutions have suffered some sort of network compromise.
  - **83%** of respondents admitted to a network compromise within the last year, compared to only **39% in 2002**.
  - **40% reported financial loss** as a result.
  - Source: vnunet.com, Date Written: May 19, 2004

Industry Turning Point

- **First Online Data Privacy Law** Looms in California. Go into effect in California on July 1. Source: COMPUTERWORLD, June 28, 2004

Law On Public Notification

- **Cyberspace Invaded**
  - Antivirus researchers have uncovered … an **underground economy specializing in identity theft and spam**.
  - Those Web servers are then used to host everything from pornography and **pirated software sites to fake banks**
  - Viruses and worms carrying Trojan horse code are also powering massive **identity theft rings**.
  - Source: COMPUTERWORLD, August 30, 2004

IT Press Aware

- **Crooks slither into Net's shady nooks and crannies**
  - Organized crime rings and petty thieves are flocking to the internet like start-ups in the go-go '90's, federal authorities say – establishing a multibillion-dollar underground economy in just a few years.
  - Source: USA Today, Date: Oct 21 2004

- **Unprotected PC's Can Be Hijacked In Minutes**
  - Automated cyberattacks saturate net, Unprotected PC's compromised in 4 minutes!
  - Source: USA Today, Date: November 30, 2004

Public Press Aware

- **Putting an End to Account-Hijacking Identity Theft**
  - FTC has estimated that almost 2 million U.S. adult Internet users experienced this fraud during the 12 months ending April 2004. Of those, 70 percent do their banking or pay their bills online and over half believed they received a phishing e-mail.
  - Source: Federal Deposit Insurance Corporation, Division of Supervision and Consumer Protection Technology Supervision Branch, December 14, 2004

Regulators Aware

The Story Keep Getting Better…

- **Bank of America Corp. lost computer tapes containing personal information on 1.2 million federal employees, including some members of the U.S. Senate.**
  - lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft.
  - Source: CBS, February 25, 2005
- **Lexis Nexis Breach Signals Bad-Security Trend**
  - Hackers gained access to the personal information of as many as 32,000 people
  - Source: News Factor Network March 9, 2005
- **ChoicePoint, a company that sells personal data to governments and businesses, reported that thieves had gained unauthorized access to its data on 145,000 consumers in the United States.**
  - data include names, addresses, Social Security numbers and credit reports. ChoicePoint said the thieves set up fake companies to get access to the data.
  - Source: Gartner Research February 22, 2005
- **Kaiser Permanente patient data exposed online**
  - A disgruntled former employee at Kaiser Permanente, posted a link to a Web site containing the personal information of 140 Kaiser patients -- an effort, she said, to call attention to a potential breach of privacy laws by the company.
  - Source: Computerworld, March 16, 2005
- **More Than 1 Million Bots On The Attack**
  - At least a million machines are under the control of hackers worldwide, said security experts in Germany (machines are used to launch attacks remotely)
  - Source: InformationWeek, March 16, 2005
- **Personal information from more than 8,900 people was stolen when thieves broke into a Nevada DMV office**
  - Source: ASSOCIATED PRESS March 11, 2005
- **Feds Rule Banks Must Tell Customers Of Security Gaffes**
  - Four federal agencies this week issued rules to U.S. banks that require them to inform customers when their personal data has been made public because of a security breach.
  - Source: InformationWeek March 25, 2005

The Problem: Client Risk is Dramatically Rising

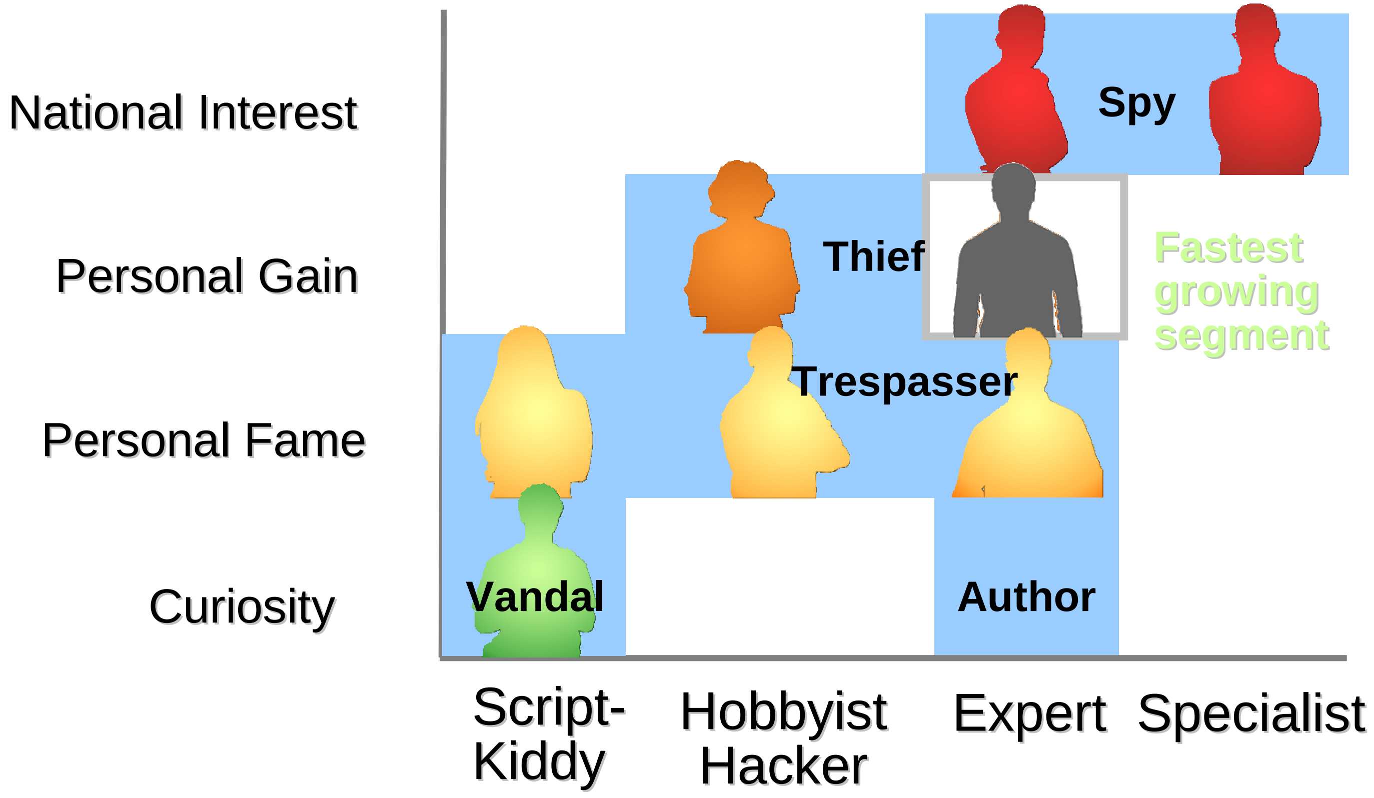
- The number of attacks in the wild, and their lifetimes and impact are growing fast
  - 450% increase in Windows viruses over last year
  - 1500% growth in BotNets Jan to Jun 2004
  - The myDoom.O virus overloaded networks around the world in August 2004
  - Blaster worm attack cause First Energy's Davis Besse Nuclear Reactor to loose digital control for over four hours in January 2003
  - Viruses are already deploying attacks against AntiVirus software
  - 80% of clients have spyware infestations
  - 30% of clients already have back doors

Source: IBM Industry Solutions Center,
Watson Research Lab.,Hawthorne, NY,
November 16, 2004

- Businesses pay $48 billion a year to clean up after ID theft schemes.

  Ken Hunter - President and CEO, Council for Better Business Bureaus, November 28, 2004

Understanding the Landscape



"Why do you rob banks?

Because that is where the

Money is"… Willie Sutton

1920's Bank Robber

So again, why are criminals on

the internet? …

Source: David Aucsmith, Architect and CTO
Security Business Unit, Microsoft Corporation
May 18, 2004

Security trends

- The State of Information Security, 2004 ***A Worldwide Study Conducted by* CIO *Magazine and PricewaterhouseCoopers***
  - Online from March 22 - April 30, 2004.
  - *CIO* and *CSO* magazines, clients of PWC, 62 countries, cross industry
  - > 8,100 CEOs, CFOs, CIOs, CSOs, VP, Dir. of IT and information security, 62 countries, margin of error 1 %.
- **Findings:**
  - Spending: Information security budgets remained flat with 2003, but went up as a % of IT (10.93 % in 2003 to 11.27 % in 2004) FSS 9.9%. Spending is getting smarter.
  - Security Breaches/Incidents — The Hits Keep Coming, But the Damage Is Being Minimized (so far)
  - **Drivers: Government regulations and potential liability the biggest factor driving security**
  - Security spending may be occurring in departments other than IT such as finance in order to comply with Sarbanes Oxley, Patriot Act etc.
  - Governance: Reporting structure shifting, more senior-level security positions and the security organization more frequently reports outside of IT (risk management (8% vs. 2% in 2003), internal audit (9% vs. 4% in 2003), legal counsel (4% vs. 1% in 2003) and security committee (7% vs. 3% in 2003)).
  - Physical security and logical security are merging at an increasing rate.
  - Information security professionals in large part did not execute this year what they said last year were their top strategic priorities.

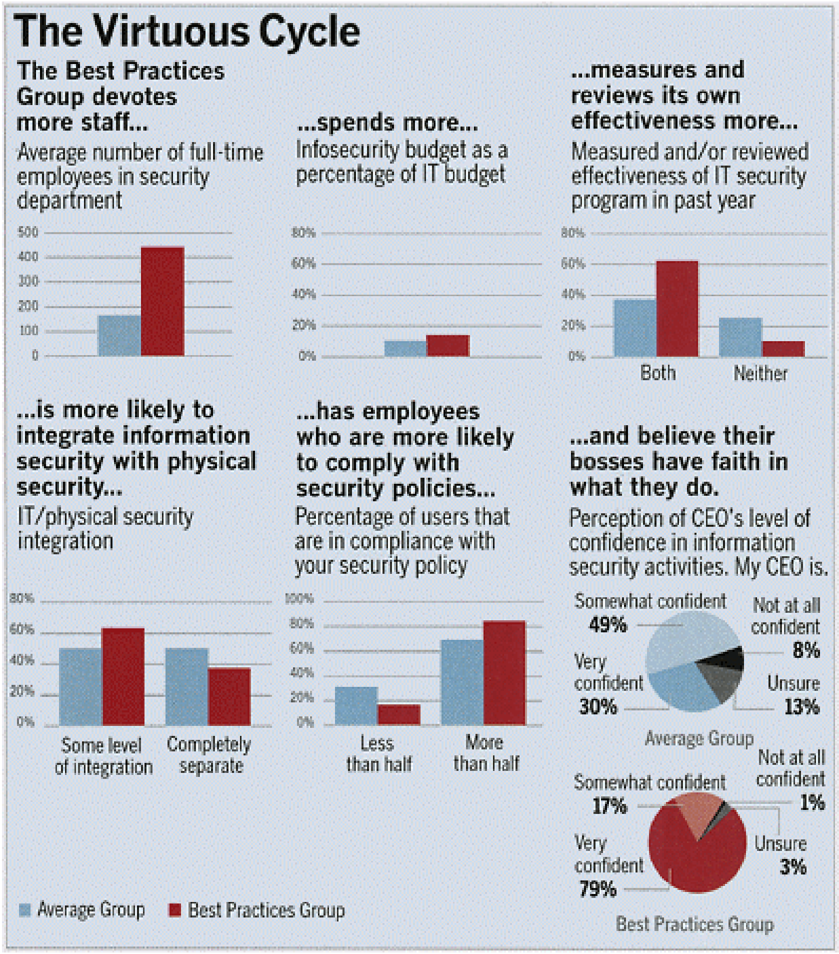
The Best Keep Getting Better

The Six Secrets

- 1. **Spend more**. U.S. respondents said infosecurity accounts for less than 9 percent of their IT budgets. (Globally, it's 11 percent.) The Best Practices Group claimed 14 percent.
- 2. **Separate information security from IT and then merge it with physical security.** These disciplines can either exist under a single CSO or as separate entities governed by an executive security committee.

Over the course of the next year:

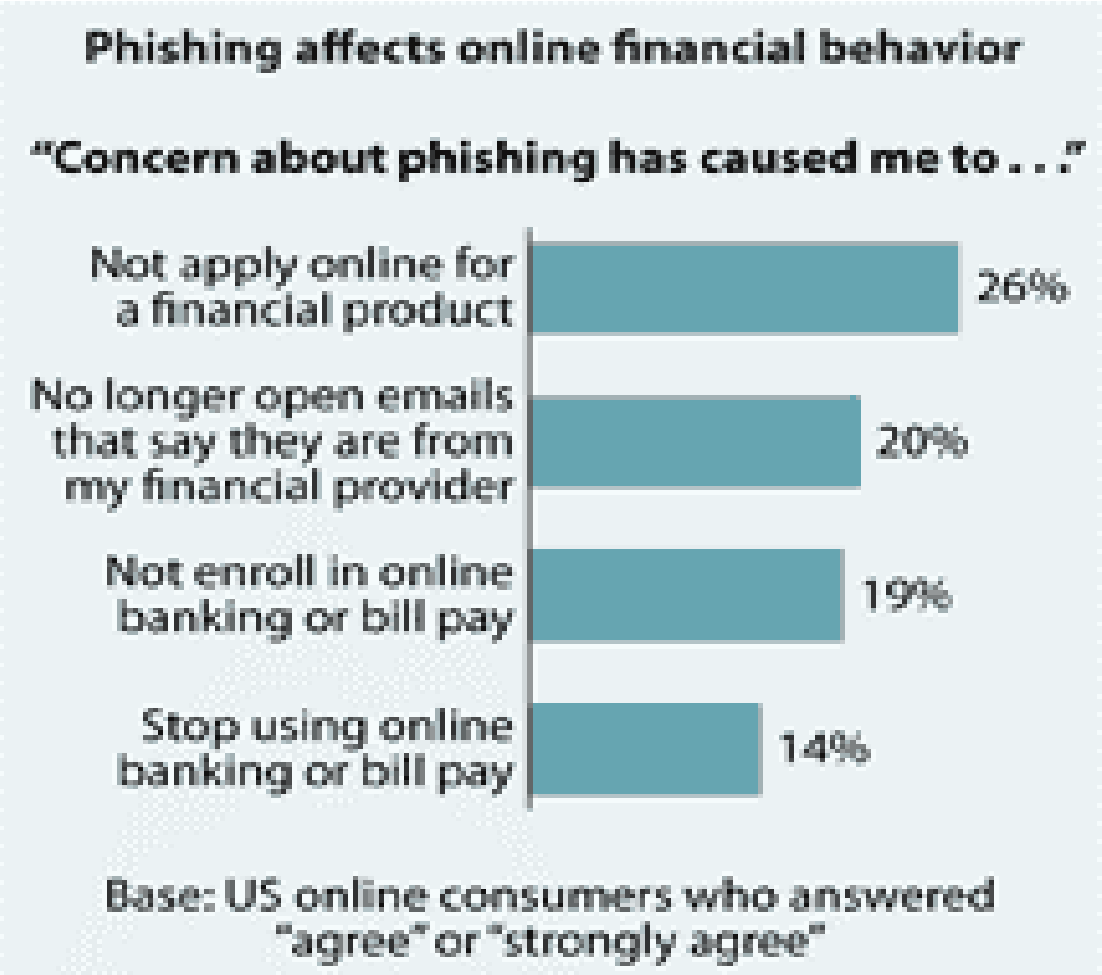
- 3. Conduct a **penetration test** to patch up network and application security (the Best Practices Group was 60 percent more likely to do this than the average respondent), and perform a complete security audit to identify threats to employees and intellectual property. (The Best Practices Group did this far more often than the average respondent.)
- 4. Create a comprehensive **risk assessment** process to classify and prioritize threats and vulnerabilities. (The Best Practices Group was 50 percent more likely to do this.)
- 5. **Define your overall security architecture** and plan from the previous three steps. (Two-thirds of the Best Practices Group did this as opposed to only half of the respondents overall.)
- 6. Establish a **quarterly review process, using metrics** (for example, employee compliance rates) to measure your security's effectiveness. This will help you to use your increased resources more efficiently.



FORRESTER

Financial Services First Look

Research & Event Highlights From Forrester



December 2, 2004
Phishing Concerns Impact Consumer Online Financial Behavior
by Catherine Graeber
with Ron Shevlin, Adele Sage

Deloitte Touche Tohmatsu predicted (01/28/05) that digital crime and online security threats will **skyrocket in 2005** as a result of the rapid growth in portable Internet and mobile technology.

The Regulatory Environment…

- **Quotes:**

  - **Whether regulation or market forces will prevail** in the public debate about electronic identity theft may be **decided in favor of legislation** this year as lawmakers react to a series of high-profile thefts involving personal information from data aggregators such as ChoicePoint and the LexisNexis Group.
  - Federal lawmakers have introduced **18 cyber security bills** and state legislators have offered **30 bills** to deal with growing online threats stemming from spyware, phishing, spam and other pernicious activities on the Internet.
  - Coviello said he favored more widespread adoption of **known industry best practices** such as encrypting stored data and using strong authentication to control access to online information.
  - Those pieces, he said, include setting standards for stronger core documents such as driver's licenses that establish a person's identity, improving the technology that links to those documents and creating incentives for people to replace weak pin and password security with stronger two-factor authentication.
  - "We need to move quickly if we're going to preserve the benefits of the Internet for commerce," James said.
  - Coviello echoed that concern, saying that **"for the first time, we actually run the risk of going backward on the Internet** because of the level of fraud" that now exists. **Source:** ID theft stirs lawmakers, FCA, April 15, 2005

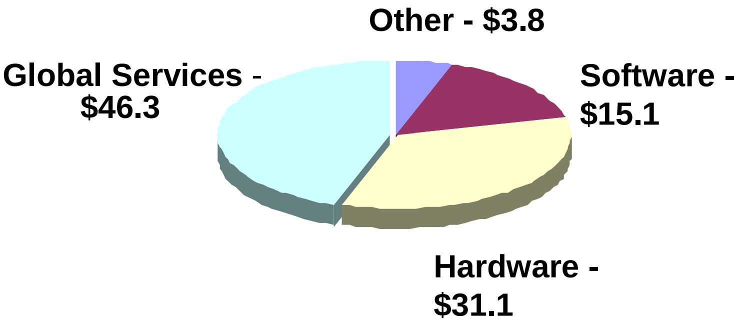
  - "**Legislation will now come**. The FTC (**Federal Trade Commission**) has asked for external authority to cover all CO's. I think they will get it.“ **Source**: John Brady, Head of Security Visa International, April 14, 2005

IBM at-a-glance

- **A global company**
  - Corporate headquarters: Armonk, NY
  - Serving customers in 160 countries worldwide
  - Nearly 60% of revenue generated outside the United States

- **The world’s largest information technology company and the 8th largest corporation in the world**

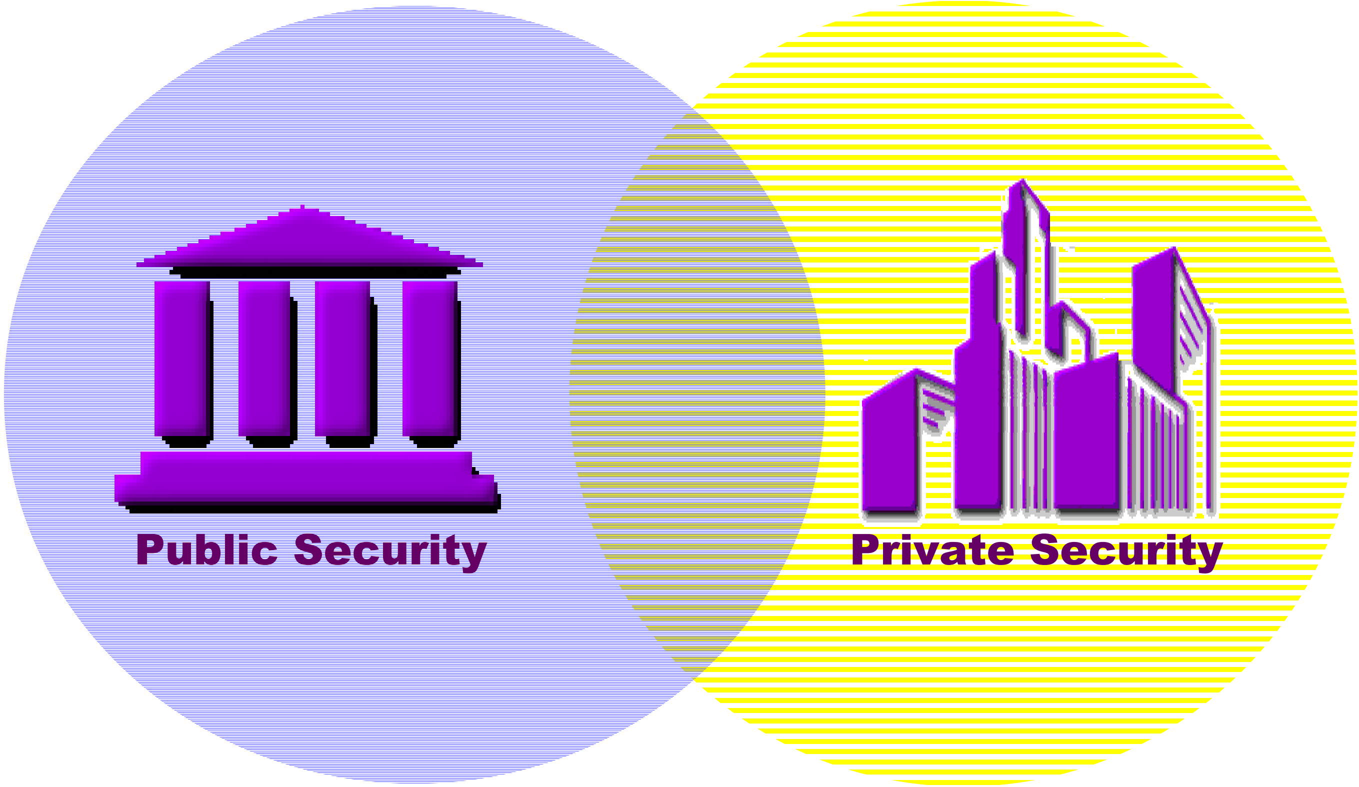
- **Year end 2004, IBM reported:**
  - $96.3 billion in revenue
  - $8.4 billion in net income
  - More than 329,001 employees worldwide
  - For the 12th straight year more US Patents then any other company world wide
  - Over 2,500 Patents in security



What keeps my customers awake at night?

- Increasing need to comply with **“unfunded mandates”** being driven by **federal regulations** (i.e. HIPAA, GLBA, AML, Sarbanes-Oxley, etc)
- Lack of qualified “safety and security” **resources** and difficulty retaining those already on staff
- Rapidly **increasing threat** to the organization’s IT environment from viruses, worms, and other malicious content exploiting their countless (and often unknown) vulnerabilities
- **Physical safety / security** concerns
- **Wireless** and new technology!
- **Economic pressures** on the organization vs. the complications associated with developing an ROI for safety/security expenditures (lack of skills in articulating value of security)

Public and Private Sector collaboration



Agenda

- **Importance of security and how it relates to regulatory compliance**
- **Security environmental changes and trends (The Bad Guys Are Winning!)**
- **IBM's leadership in the security area**
- **Regulation in the Information Age: Background**
  - What is new about regulation in the 21st century?
  - Drivers for change
  - The new regulatory paradigm: Risk-Based Supervision
- **Where are we now?**
- **The critical role of data integrity and security in the new Regulatory regime**
- **IBM Software and Services for Sarbanes–Oxley, Patriot Act, GLB etc.**
- **Summary**

The Industrial Age approach to regulation is out of step in the Information Age

Traditional Regulatory Regimes

- Static focus
- highly prescriptive and rules-based
- Compliance is siloed and risks stand alone
- Compliance functions typically low level and dispersed throughout organizations
- Regulation viewed as exclusively the concern of the government
- Focus on discrete violations and correction of those violations

Shortcomings

- Inflexible and unable to keep up with rapid change
- May not capture risk appropriately
- Dependencies not adequately assessed
- Can encourage “gaming the system” (e.g. Enron)
- Highly labor intensive and slow

Traditional system failed to recognize early warning indicators for the Enron, WorldCom, Parmalat, BCCI, Barings Bank, Vivendi, etc.

21st Century drivers enhance competitiveness while heightening systemic risk and evolving exposures

1. **Globalization**
   - The global economy has become a reality
   - Concept of boundaries is less clear
   - Interdependence of global markets exacerbates contagion risk
   - Threat of international terrorism
2. **Deregulation & Consolidation**
   - Deregulation fosters freer play of competitive forces
   - Fosters development of multinational conglomerates that are challenging legal and regulatory jurisdictional boundaries
   - Industry consolidation raises unprecedented levels of risk / concentration of systemic risk in fewer companies
3. **Technological advances**
   - Technology rapidly changing products, processes, and capabilities – business becoming increasingly complex
   - Critical infrastructure sophistication and vulnerability
   - Heightened security and privacy concerns for data and people

These drivers are forcing a sea change in regulatory focus, approach and implementation…

Focus

- **Proactive**: Anticipate vulnerabilities
- **Global**: Regulations have global impact
  - Jurisdictional sovereignty must be rethought
  - Legal and cultural clashes are inevitable and must be reconciled
- **Comprehensive**
  - Recognize new players and products
  - Lines of business less clearly defined

Approach

- **Nimble**: **Risks evolve and transform constantly**
  - Identification and appreciation of risk must be proactive
  - Metrics must remain meaningful
- **Collaborative:** Communication among regulators, regulated entities, and third party service providers is critical
- **Consistent:** Manage to global standards

Implementation

- **Adaptable:** Innovation and complexity rule in successful markets
  - Regulators challenged to meet fiscal and skills requirements
  - Reward innovation while mitigating risks
- **Preventative and remedial**: Terrorism risks are relatively new, unpredictable, and harmful
- **Forceful:** Price of non-compliance must be commensurate with the systemic impact

...Risk based supervision (RBS), which accommodates change and complexity and is being broadly adopted

- Looks to the future -- aim is crisis prevention
- Supervision of systemic risk by industry, firm, and customer base
- Reliance on sound risk and compliance protocols and business performance management
- Focus on corporate governance and senior management accountability -- that is documented
- Standards-based measurement of risk exposure and dependencies
- Enhanced collaboration between regulators and regulated
- Supervisory tools and intensity linked to areas of risk and concern
- Dependency on transparency, auditability, information and documentation

The new regulatory regime is information-based and information dependent

- RBS is wholly dependent on documentation and auditability
- All recent key regulations require establishment and full documentation of internal processes, and strict data management
- Data security, authenticity, retention, retrieval, backup, and auditability capabilities are issues being driven by Sarbanes-Oxley, Patriot Act, Basel II risk management assessments, and the renewed concern about operational risks

Agenda

- Regulation in the Information Age: Background
- Where are we now?
- The critical role of data integrity and security in the new Regulatory regime

The impact of recent corporate scandals combined with the 9-11 attack accelerated regulatory transformation and supervisory urgency

- Confidence in US and global markets severely shaken
  - Risk of global economic depression
  - Exposed dire need for consumer protection
- New regulations rapidly adopted to shore up capital markets and protect consumers
- Enforcement penalties severe and personal
- Privacy and security issues now in the forefront
- Critical infrastructure protection a major concern

Regulatory response has been swift and far reaching…

- Basel II
- Sarbanes-Oxley
- Patriot Act
- Gramm-Leach-Bliley
- California Financial Information Privacy Act
- IMF Financial Sector Assessment Program

……..but regulatory action alone is not enough to stem the tide

Rapidly evolving fraud challenges threaten the safety and security of financial markets and shake consumer confidence

Identity Theft

27.3 million consumers have been victims of identity theft over past 5 years, with 9.9 million in the last year

Losses to businesses are estimated at $48 billion, with consumers reporting $5 billion in out-of-pocket expenses

(FTC, 9/03)

Misclassification of Fraud Losses

Gartner projects more than two-thirds of fraud will be misclassified as credit risk in 2004

Banks suffer higher risk ratios since Credit Losses are not insured which leads to higher capital reserve costs under Basel II

(Gartner, 5/04)

Phishing

Direct losses from identity theft against phishing attack victims cost US banks and credit card issuers $1.2 billion in 2003

(Gartner, 5/04)

Internal Fraud

Internal fraud believed to cost US financial services firms up to $2.4 billion in 2004

(Celent Communications)

Criminal attacks on data security are becoming more frequent, more costly, and more ingenious, causing data governance and security to be of paramount – and growing concern

- Hacking
- Denial of service
- Identity theft and fraud
- Intrusion and extrusion breaches
- Phishing
- Pharming
- Skimming

Let’s consider a couple of today’s greatest challenges

Now that we're wise to phishing, pharming is emerging

- **Phishing**
  - **Scammers lure users into disclosing personal data through fake email and websites that look like they belong to actual companies**
  - **Cost to consumers in 2004 estimated at $500M (average $115 per victim)**
  - **Phished poster children include eBay, Citibank, PayPal – even the FDIC!**
  - **Public is on the alert now**
- **Pharming**
  - **A variation on domain spoofing, a relatively old concept often used by hackers/crackers to direct denial-of-service attacks**
  - **Pharmers poison local DNS servers to redirect Web requests to a different site without the knowledge of, or action by, the user**
  - **In January, 2005, the DNS address for the domain panix.com, a NY State Internet service provider was fraudulently changed. Ownership of the company was changed from New York to Australia; requests to reach the panix.com server were redirected to the UK, and e-mail was redirected to Canada. State and Federal authorities are currently investigating this case**

Source: Robert Vamon, CNET Review, February 18, 2005

And extrusion breaches are taking prominence over intrusion

- Extrusion:the unauthorized transfer of essential digital assets such as credit cards, customer records, transactional information, source code, and other classified information
- Term coined by Tim Sullivan of Fidelis Security, as shorthand for “trusted insider theft over the network”
- Regulation is a major driver in implementation of extrusion prevention
  - Sarbanes Oxley and corporate governance

    Section 404: “Management Assessment of Internal Controls”

    Section 409: “Real-time Disclosure”

  - Basel II: Operational Risk

Online banking fraud is rising and exposing banks to serious operational and reputation risk

- Online Banking Fraud**:** the criminal compromise of a legitimate customer’s online banking account for the purpose of transferring money out of the account via a number of available channels

- Financial and operational impact is severe
  - While the financial impact varies widely, customers typically lose the entire contents of their DDA accounts.
  - The secondary effect of online banking fraud is to undermine consumer confidence in an important, low cost new channel.
- Abrupt change in behavior patterns point to online banking fraud, but stronger authentication could prevent it
  - By monitoring and profiling the normal behavior of accounts, it is possible to identify abnormal, risky behavior using sophisticated models trained on past legitimate and fraudulent transactions.
  - Once elevated risk is detected, usually two interventions follow: first, risky transactions may be delayed in many settings. Second, human review and verification are normally the final intervention and decision point for acceptance or rejection of an on-line transaction.

Agenda

- **Regulation in the Information Age: Background**
- **Where are we now?**
- **The critical role of data integrity and security in the new Regulatory regime**

Data security and management is a key imperative cutting across all major regulatory initiatives

- Government's hands-off approach to regulating security just reversed course. Homeland security will serve as a publicly acceptable excuse to increase overall governmental supervision of business. ..The impact of international rules regarding money laundering, privacy and security will spread from financial services to other industries, regardless of jurisdiction.
- .. Enterprises that adapt swiftly to the new environment will find unanticipated benefits. Increased security and privacy regulation will flood customer relationship management (CRM) initiatives with new information about customers, information that might be capitalized on—at least in the United States—as organizations get to know their customers more intimately. Tightened security and privacy measures will also be a strong, value-added selling feature for an increasingly cautious customer base in search of a trusted supplier.
- **Data protection is becoming a worldwide regulatory issue**
- Concerns about security and privacy are spreading from financial services to every industry. Moreover, the playing field is changing: **Privacy is no longer just a local best practice—it's becoming a global regulatory issue.** (emphasis added)

Richard DeLotto, Gartner Group

Even the SEC – the Sarbanes Oxley Authority -- has been called to task !

- GAO March 2005 Report: "Information Security
  Security and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data"

- Findings:
  - Failure to implement effective electronic access controls
  - Weaknesses in physical security, segregation of computer functions, application and service controls and service continuity
  - SEC has not developed and implemented a comprehensive agency information security program

- **"Information systems controls were not effective at SEC. We identified numerous weaknesses in electronic access controls and other information system controls. As a result, financial and sensitive information was at increased risk of unauthorized disclosure, modification, or loss, and operations at risk of disruption."** (emphasis added) GAO "Conclusions"

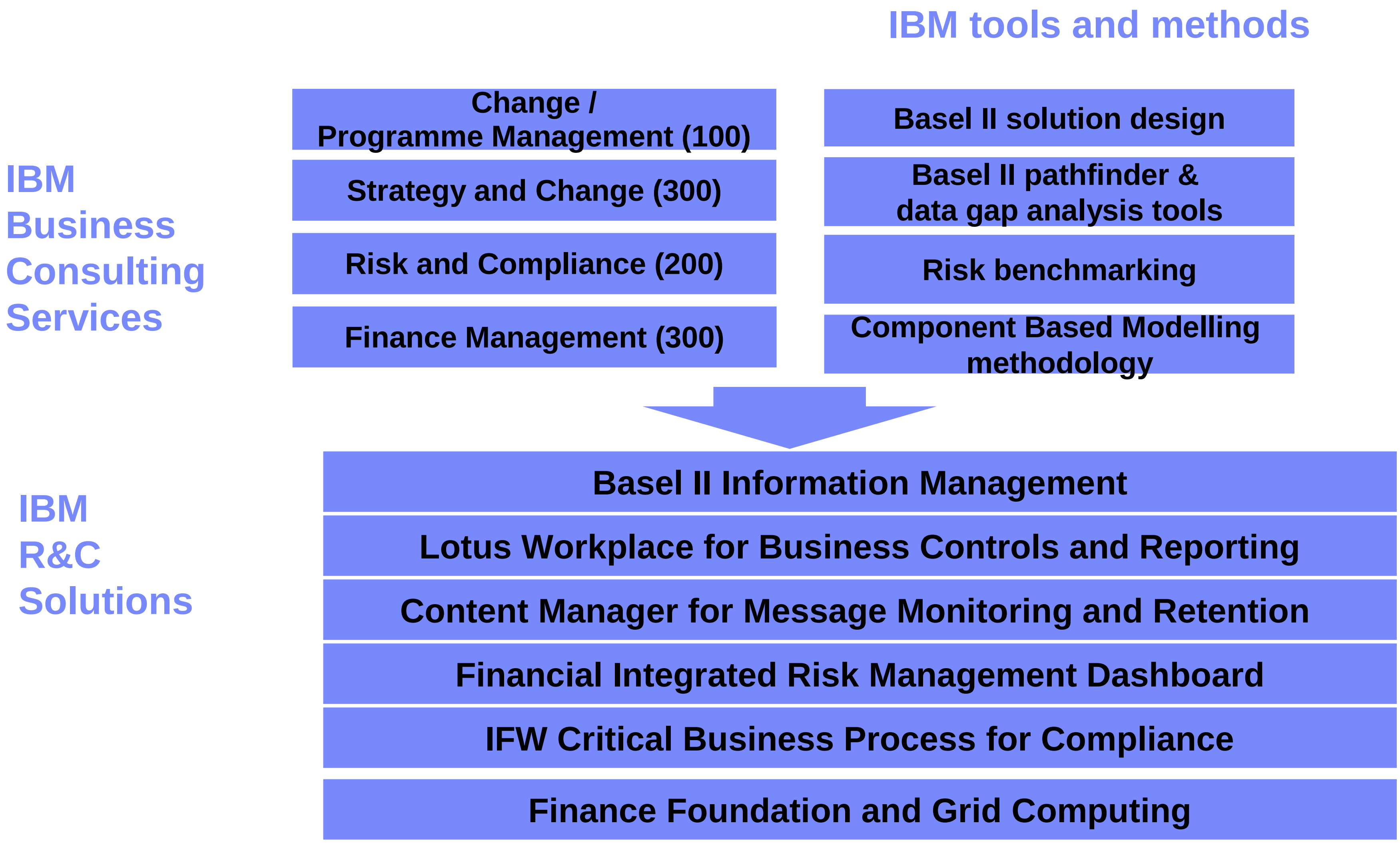
So, in summary and conclusion….

- Risk-based Supervision is the regulatory paradigm for the Information Age
- The goal of RBS is to contain systemic risk while fostering innovation
- Systemic risk is both magnified and contained by advanced technology
- Increasingly, controls that serve the dual goals of supporting innovation and limiting injurious risk are focused on the security of information and digital assets
- Regulators are looking to industry to develop and enhance controls to protect citizens and maintain secure and healthy markets

Agenda

- **Importance of security and how it relates to regulatory compliance**
- **Security environmental changes and trends (The Bad Guys Are Winning!)**
- **IBM's leadership in the security area**
- **Regulation in the Information Age: Background**
  - What is new about regulation in the 21st century?
  - Drivers for change
  - The new regulatory paradigm: Risk-Based Supervision
- **Where are we now?**
- **The critical role of data integrity and security in the new Regulatory regime**
- **IBM Software and Services for Sarbanes–Oxley, Patriot Act, GLB etc.**
- **Summary**

BCS Offerings for Risk and Compliance



IBM tools and methods

IBM Business Consulting Services

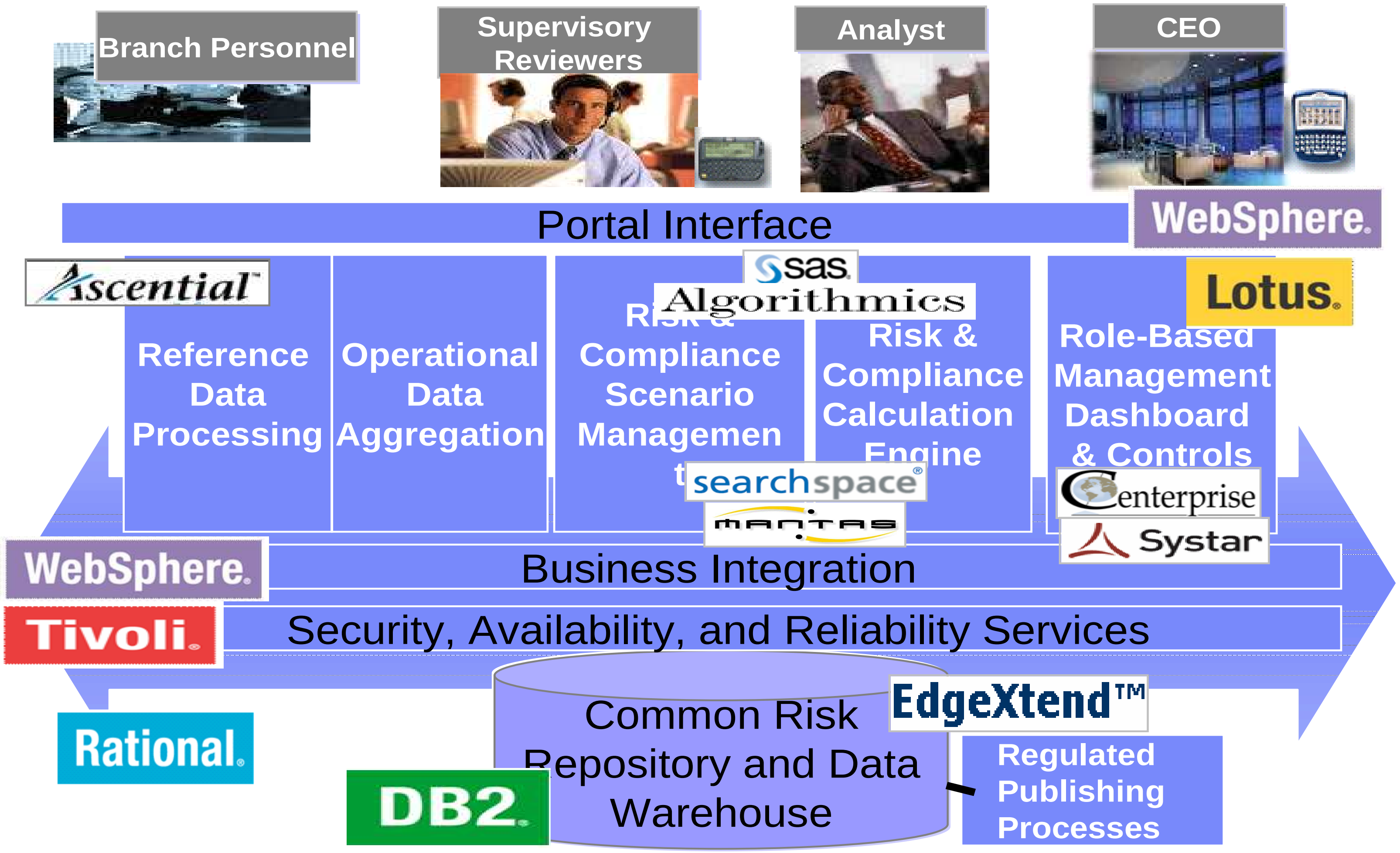
- Change / Programme Management (100)
- Strategy and Change (300)
- Risk and Compliance (200)
- Finance Management (300)

- Basel II solution design
- Basel II pathfinder & data gap analysis tools
- Risk benchmarking
- Component Based Modelling methodology

IBM R&C Solutions

- Basel II Information Management
- Lotus Workplace for Business Controls and Reporting
- Content Manager for Message Monitoring and Retention
- Financial Integrated Risk Management Dashboard
- IFW Critical Business Process for Compliance
- Finance Foundation and Grid Computing

IBM SWG Banking Risk & Compliance Offerings *Enable Management of Risk & Compliance Activities to Gain New Efficiencies*



Branch Personnel

Supervisory Reviewers

Analyst

CEO

Portal Interface

Reference Data Processing

Operational Data Aggregation

Risk & Compliance Scenario Management

Risk & Compliance Calculation Engine

Role-Based Management Dashboard & Controls

Business Integration

Security, Availability, and Reliability Services

Common Risk Repository and Data Warehouse

Regulated Publishing Processes

A Foundation for Basel II, SOX, & Anti-Money Laundering

Workplace Business Controls & Reporting

- In its design, the WBCR software leverages IBM technology and control knowledge from sources like KPMG. It provides a framework that can help extend business strategies to respond to legal and regulatory requirements.

- WBCR software as an asset and essential foundation element for your company to identify, evaluate, and report on internal business controls.
  - This offering can assist with gathering, monitoring, and organizing information about controls in a more consistent and automated manner.
  - It is a web-based, end-to-end offering that offers visibility into financial, IT, and operational controls across the enterprise.

"Easy To Use – Intuitive" / "Fits Corporate Look & Feel" / "Quick to Adapt"

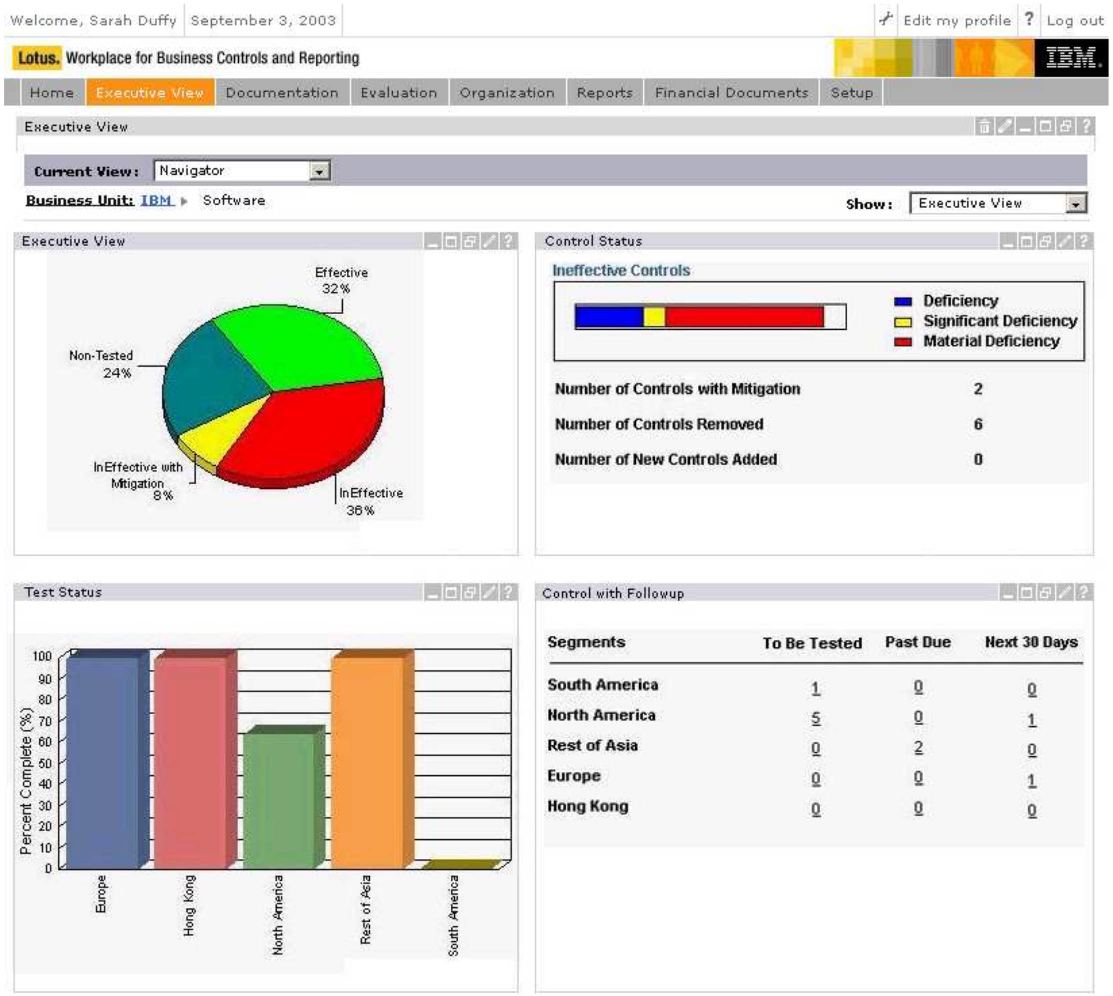
IBM Strategic Focus Drives Sustainable Compliance

- Drive Down the Cost of Compliance
  - Share controls across multiple processes to reduce testing overhead
  - Control Catalog updates to ensure consistency
  - Centralized testing capability to ease auditing and endure consistency
  - Email alerts to simplify testing process
- Simplify Testing and Auditing Processes
  - Configurable email alerts to focus employees on timely control activity
  - Automatically create samples for simplified auditing and monitoring
  - Follow trends in control history to gauge momentum and progress
  - Create more detailed access control to ensure integrity
- Ease of Alignment with your control strategy
  - Customize language in the software to match your corporate parlance
  - Customize email notifications to meet corporate control policies and timelines
  - Integrate seamlessly into your corporate intranet reducing end user training
- Accelerating exception resolution
  - Teamrooms for projects: data, plans, communications assignments, in one place
  - Expertise locator and Instant Messaging Shared
  - Customize email notifications to meet corporate control policies and timelines
- Migrate existing control data with ease
  - Enhanced import capabilities - even directly from MS Excel®
  - Import procedures directly to avoid duplication and ensure consistency across units
  - Import data with default owners

IBM Key Features

- Executive dashboard
- Versioning and archiving
- Roles and Security
- Organization Movement / Reorganization
- Controls Execution Information
- Support for manual and automated controls
- Samples and Remediation
- Certification
- Global Controls
- Email notifications
- Export Reports to Excel Spreadsheets
- Label Management and Configuration
- Support for financial and non-financial controls
- Hiding Financial Values
- Dynamic Updates
- Customized Reporting and Management Support
- Full Audit Trail
- Collaboration tools in support of test and remediation processes

IBM Workplace Business Controls & Reporting



Welcome, Sarah Duffy | September 3, 2003 | Edit my profile | ? Log out

Lotus. Workplace for Business Controls and Reporting

Executive View

Current View: Navigator

Business Unit: IBM ▸ Software

Show: Executive View

Executive View

Control Status

Ineffective Controls

- 🟦 Deficiency
- 🟨 Significant Deficiency
- 🟥 Material Deficiency

Number of Controls with Mitigation	2
Number of Controls Removed	6
Number of New Controls Added	0

Test Status

Control with Followup

Segments	To Be Tested	Past Due	Next 30 Days
South America	1	0	0
North America	5	0	1
Rest of Asia	0	2	0
Europe	0	0	1
Hong Kong	0	0	0

Transparency

- **Aggregates Information Across Enterprise**
- **Managements Snapshot of Compliance**

Consistency and Automation

- **Users Navigate Quickly to Tasks**
- **Processes are Linked to Financials**
- **Controls are Defined, Checked & Validated**

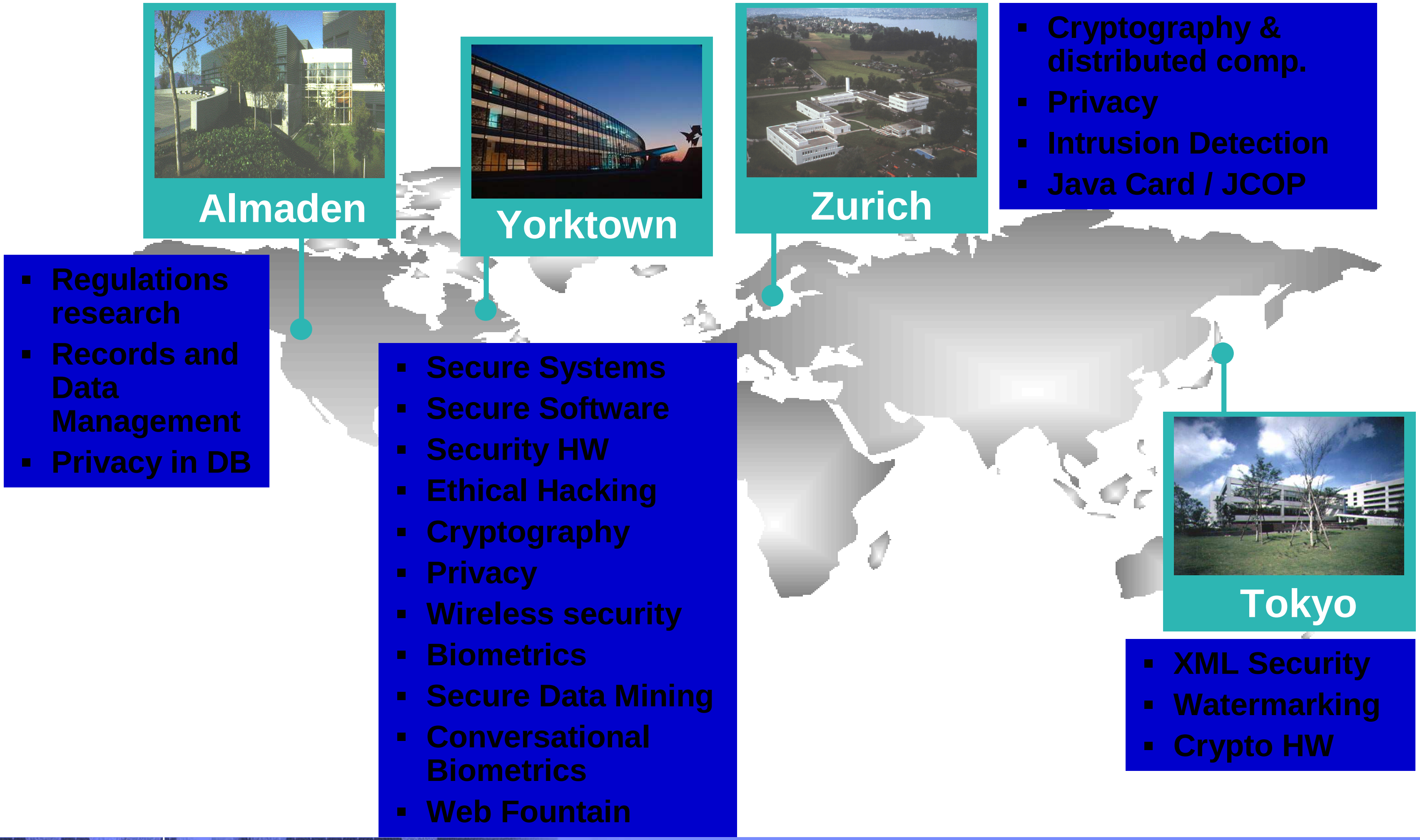
Efficiency and Effectiveness

- **Simple, Consistent Process Flow**
- **Sustainable Process and Documentation**
- **Workflow Management**

Accountability

- **Key Roles and Risks Defined by Process (CFO, Business Unit Owner, Process Owner, Control Owner, etc.)**
- **Ownership Assigned to Drive Business**

Compliance Related IBM Research Lab Projects



Almaden

- Regulations research
- Records and Data Management
- Privacy in DB

Yorktown

- Secure Systems
- Secure Software
- Security HW
- Ethical Hacking
- Cryptography
- Privacy
- Wireless security
- Biometrics
- Secure Data Mining
- Conversational Biometrics
- Web Fountain

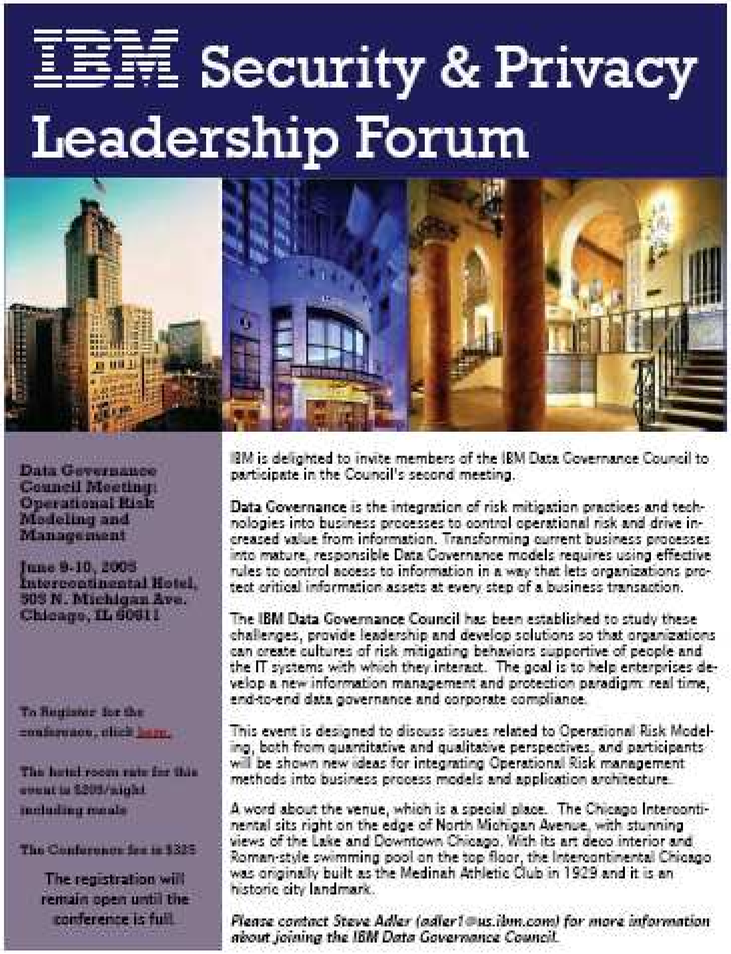
Zurich

- Cryptography & distributed comp.
- Privacy
- Intrusion Detection
- Java Card / JCOP

Tokyo

- XML Security
- Watermarking
- Crypto HW

IBM Data Governance Council Forum – June 9-10



IBM Security & Privacy Leadership Forum

Data Governance Council Meeting: Operational Risk Modeling and Management

June 9-10, 2005
Intercontinental Hotel,
505 N. Michigan Ave.
Chicago, IL 60611

To Register for the conference, click here.

The hotel room rate for this event is $209/night including meals

The Conference fee is $325

The registration will remain open until the conference is full.

IBM is delighted to invite members of the IBM Data Governance Council to participate in the Council's second meeting.

Data Governance is the integration of risk mitigation practices and technologies into business processes to control operational risk and drive increased value from information. Transforming current business processes into mature, responsible Data Governance models requires using effective rules to control access to information in a way that lets organizations protect critical information assets at every step of a business transaction.

The IBM Data Governance Council has been established to study these challenges, provide leadership and develop solutions so that organizations can create cultures of risk mitigating behaviors supportive of people and the IT systems with which they interact. The goal is to help enterprises develop a new information management and protection paradigm: real time, end-to-end data governance and corporate compliance.

This event is designed to discuss issues related to Operational Risk Modeling, both from quantitative and qualitative perspectives, and participants will be shown new ideas for integrating Operational Risk management methods into business process models and application architecture.

A word about the venue, which is a special place. The Chicago Intercontinental sits right on the edge of North Michigan Avenue, with stunning views of the Lake and Downtown Chicago. With its art deco interior and Roman-style swimming pool on the top floor, the Intercontinental Chicago was originally built as the Medinah Athletic Club in 1929 and it is an historic city landmark.

Please contact Steve Adler (adler1@us.ibm.com) for more information about joining the IBM Data Governance Council.

IBM Advantage / Differentiators

- Minimizing Cost for Managing Risk & Compliance
- Stepped Approach for Compliance Challenges
  - ✓ Start with 404 controls, expand into modelling / improvements into Financial Business Processes
  - ✓ Add 802 Archiving / Retention
  - ✓ Move to 409 (speed 10k/10Q creation), address real-time material event reporting
- Common Infrastructure Framework leveraged for Multiple Risk & Compliance Initiatives
  - ✓ Consistent / Easy-to-Use Experiences
  - ✓ Real-Time Information for Decision Makers
  - ✓ Readiness Status – At a Glance
- 24 x 7 x 365 Standard Software Support

IBM Differentiators

- Global Scale and delivery capabilities: world's largest software organization
- Integrated services; strategy through implementation and operation
- Deep industry expertise and knowledge of industry processes
- Leading-edge Solution Focus on SOX and other risk & compliance areas
- Deep technology skills
- Strategic alliances with leading technology vendors
- Premier client list and "track record" of success
- Focused investment in innovative solutions, people development, and intellectual capital

Why IBM

Market Observations	IBM Value Proposition	Differentiation
Compliance is a part of the larger security and privacy system	IBM has the experience and expertise with integrating secure identity into complex systems	Most secure vendors don't understand the total security and privacy picture
Security systems are by definition human-centric	IBM has consulting, training, and management capabilities that are key to secure identity projects	Most secure vendors are focused only on their technology area
Security technologies will improve significantly	IBM has experience with enterprise architectures and change management processes	Most secure vendors don't appreciate total cost of ownership issues
Security companies will continue to see consolidation	Customers want a trusted business partner like IBM, not a small technology vendor	Many of today's secure vendors will not be around in a couple of years

IBM Safety, Security & Privacy web sites

- **IBM Safety & Security (external):** www.ibm.com/security
- **Security and Privacy Services:** www.ibm.com/services/security
- **Security Health Check:** www.ibm.com/services/security/scrspec.html
- **Business Continuity and Recovery Services -** www.ibm.com/services/continuity/recover1.nsf/documents/home
- **Tivoli security products -** www.tivoli.com/products/solutions/security/news.html
- **Secure clients -** www.pc.ibm.com/ww/security/index.html
- **e-Server systems -** www.ibm.com/servers
- **PCI Cryptographic Coprocessor -** www.ibm.com/security/cryptocards/index.shtml

ibm.com/services/security

Priscilla Rabb Ayres
rabbayres@us.ibm.com
202.515.5156

Bob Kennedy, CFP, CISSP
rjkenned@us.ibm.com
732.384.2566