Emerging technology and its impact on GRC

Represented by
Dr. Yeffry Handoko Putra, M.T
Indonesia Computer University

Today's Agenda

Introduction to guest presenters & housekeeping

Emerging Technology & Impact on GRC

Emerging Technology Spotlight

- Surveillance and Monitoring
- New Payment Technology
- Bring Your Own Device (BYOD)
- Big Data
- Cyber Security
- IP Protection & Information Privacy

The future of GRC – delivering ROI in times of increased risk:

New KYC Paradigm and GRC technology

Questions

Housekeeping

- Presenters will introduce key technology themes
- Discussion after each theme
- Please send in any questions you have via Go-To chat and we will have the panel address them
- There should be time for a Q&A at the end

Emerging Technology & Impact on GRC

Technology is changing the way businesses and individuals are interacting, communicating and sharing information.

- Nearly a billion people used Facebook in June 2012
- Twitter generates over 200 million tweets per day
- 100 billion searches are generated each month via Google
- The volume of business data worldwide doubles every 1.2 years

58% of audit professionals identified risk around **information data privacy & security** as causing them the most angst

28% identified **social media** (impact on reputation & customer strategy)

What challenges are GRC professionals facing?

Key governance concerns include:

- Accelerating global regulations – FATCA, FOFA, Code of Banking Practice, Financial Claims Scheme, Basel III and AML, ABC
- Governance, processes & control
- IT Risk and emerging technologies – new payment methods
- Information Privacy/Security and Cyber-Security

felt satisfied that their company's governance process and controls are keeping pace with technological change.

Sources: *Deloitte Bribery & Corruption Survey, AU & NZ, 2012; Is Governance Keeping Pace? KPMG, Audit Committee Institute 2012*

Emerging Technology Spotlight

- Surveillance and Monitoring
- New Payment Technology
- Bring Your Own Device (BYOD)
- Big Data
- Cyber Security
- IP Protection & Information Privacy

Surveillance & Monitoring

CONTEXT

- Omnipresent technology connected to the web is the ultimate panopticon
- Almost everyone carries a device which constantly sends information about that person's location (via GPS), activities and interactions
- Growing adoption of employee monitoring tools: keystroke monitoring, email logs, web activity, etc

THREATS & RISKS

- Millions of transactions occurring each day; need sophisticated transaction monitoring systems to identify unusual or suspicious behaviour
- Internal monitoring – emails and internal trading to ensure compliance with trading blackouts etc
- Surveillance is most likely restricted by law – but often the legal framework is ambiguous.
- Surveillance may be required by law!
- Significant risk of breaching employee privacy
- Impact on employee morale

REDUCING THE RISK

- Deploying state of the art transaction monitoring systems – configuration of rules by subject matter experts and extensive tuning / fine tuning
- Regular review of TMP effectiveness – which rules have fire and never fired
- Ensuring compliance with policies and procedures – breach monitoring and
- Ongoing oversight and independent reviews
- Using social media monitoring tools to detect insurance fraud
- Effective due diligence – KYC/KYE

CASE STUDY

· Use of data analytic tools to mine data to support criminal investigations – corporate collapses such as Enron, email analytics between main players

New Payment Technology

CONTEXT

- New technology emerging with contactless payment systems such as credit cards and debit cards, key fobs, smartcards or other devices that use radio-frequency identification (RFID) for making secure payments
- According to RBA statistics, there are an estimated $470 million dollars in cash transactions under $35 moving through the Australian economy each day, or around $170 billion per year
- Technology to be adopted by businesses in 18-24months

Forms:

- Contactless cards – go money and pay wave
- Peer to peer payment via mobile phone
- Kaching

THREATS & RISKS

- The RFID chip feature comes switched on, and can't be switched off. The consumer has no choice - the card comes with the functionality
- No authentication is performed of the authority of the person to use the card (i.e. no signature, no PIN).
- Transactions may or may not involve visual notification to the cardholder, who may or may not notice any such display
- Data privacy concerns (over-collecting information)

REDUCING THE RISK

- Know your limits
- Be app savvy
- Put security measures in place
- Wipe your old phone

CASE STUDY

Use of digital currency account to facilitate Internet fraud and money laundering

A young person, acting as a nominee, opened a digital currency account to enable him to receive the proceeds of Internet banking thefts from an offshore associate. He then attempted to redeem the value of the digital currency account by requesting the digital currency exchanger to provide him with postal money orders. In an effort to conceal his identity he informed the cash dealer that he had lost his passport and requested that the exchanger call a money service business and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted.

Bring Your Own Device (BYOD)

CONTEXT

- BYOD refers to employees bringing their own computing devices – such as smartphones, laptops and PDAs – to the workplace for use and connectivity on the corporate network
- BYOD is about a mobile and flexible working environment which offers significant productivity enhancements for "on-site" GRC tasks (e.g. OH&S, food safety, environmental inspections, etc.)
    - 80% of employees used own devices at work
    - 53% of companies condone BYOD
    - 63 % of employees believe BYOD positively influences their view of the company

THREATS & RISKS

- Data loss or leakage (assuming a device is stolen/lost without being backed up and secured)
- Data held on personal devices might be discoverable. (When someone participates in a BYOD program everything an employee does on her personal iPhone, for example, could be used as evidence in a lawsuit against her employer.)
- Who's responsible for Repetitive Stress Injuries from the use of a BYOD device?
- Shared devices – how secure is corporate data from an employee's partner or housemate?
- Unsafe disposal of devices (i.e. hard drive tossed without being wiped)
- Impact on individual's content (e.g. personal photos) if device is wiped by action of another company employee

REDUCING THE RISK

- Remote locking / deleting of devices – wiping iPhones remotely
- Mobile Device Management (MDM)
- Education

CASE STUDY

2011: Eighteen months ago a financial services firm (Blackstone) allowed employed to use iPads. Today, there are some 600 iPads among nearly 2,000 employees that tap the corporate network for confidential documents and emails. Most of them are privately owned BYOD devices. Issues around how to slove IP security. Problem solved through central mobile device management such as Mobileron and WatchBox.

Big Data

CONTEXT

- Big data is a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications

"It's important to recognise that this is an information revolution more than a technology revolution"
KPMG Audit Committee Institute Report, 2012

Big data will be a key driver of innovation, productivity, competition and transparency

THREATS & RISKS

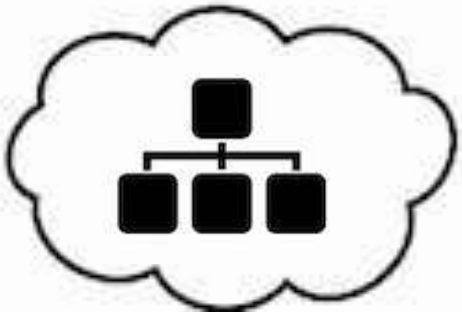
- Tools which enable more sophisticated data mining and pattern analysis mean that it is possible to identify 'interesting' information that was previously unattainable
- Wasting money
- Databases are not free – how to ensure ROI on Big Data projects?
- Privacy breaches
- Copyright infringement

REDUCING THE RISK

- Governance!
- Obtain consents
- Anonymise
- Identify and avoid or secure "toxic data". E.g. credit card numbers
- Third part content (copyright)
- Data handling policies and policing
- Effective due diligence process - KYE

CASE STUDY

- Wikileaks – published tens of thousands of classified military documents
- Industrial espionage – stealing trade secrets and designs etc.
- Facebook has hundreds of millions of users and sensitivities of data loss
- Kim Dotcom – piracy of documents via Megaupload



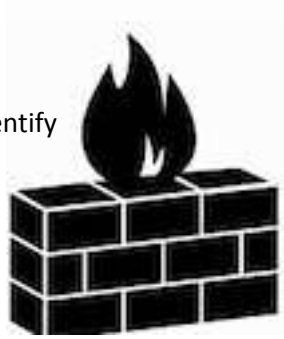
Cyber Security

CONTEXT

- Information security as applied to computers and networks
- The *2012 Cyber Crime and Security Survey Report*, commissioned by CERT Australia, revealed that cyber attacks are now more coordinated and targeted for **financial gain**
- **Cost of cybercrime $5bn** per year and growing
- SMEs reported individual loss of $650m due to cybercrime
- 44% of attacks originating from within organisations

THREATS & RISKS

- Most common form of cyber security issue is actually theft/vandalism by current/former employees
- Cloud based storage raises additional risk as **data is held by a third party and potentially stored in a foreign jurisdiction** (the US Patriot Act has raised concerns in the Pacific Region)
- Denial of service attacks can be problematic for businesses with heavy online presence or critical business functions using a web interface
- Breach of confidentiality information
- Millions of transactions occurring each day; need **sophisticated transaction monitoring systems** to identify unusual or suspicious behaviour
- **Internal monitoring** – emails and internal trading to ensure compliance with trading blackouts etc.



REDUCING THE RISK

- Ensuring firewalls are in place to protect data
- Email blockers for filtering out spam emails
- Ensuring employees are unable to download software files from unknown sources
- Preventing employees from accessing certain websites
- Informing customers of the importance of protecting their identities
- Deploying state of the art transaction monitoring systems –
- Effective due diligence – KYC/KYE/KYS
- Regular review of TMP effectiveness – which rules have fire and never fired
- Ensuring compliance with policies and procedures – breach monitoring
- Ongoing oversight and independent reviews
- Using social media monitoring tools to detect insurance fraud

CASE STUDY

SEPT 2012: CERT Australia receives calls from more than 25 organisations being targeted by ransomware.
> The attacks encrypted files on the compromised system and/or locked victims out of the desktop environment.
> The attacks also encrypted files in the system backups.

The victims were then asked by the attacker to pay a fine using a payment or money transfer service, to obtain the codes that would unlock the computer and/or decrypt the data.

DATA MINING: Use of data analytic tools to mine data to support criminal investigations – corporate collapses such as Enron, email analytics between main players

Intellectual Property & Information Privacy

CONTEXT

- Intellectual Property (IP) Protection and Information Privacy are closely linked
- IP is an important asset in today's knowledge economy and should be strategically managed

THREATS & RISKS

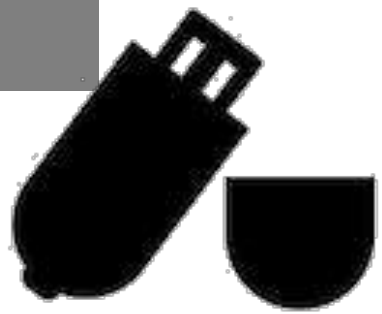
- Not differentiating between personal information that is required by law to be collected and information that is not
- A 'collection notice' is not provided (as is required by Australian law)
- Sensitive information is collected but is not recognised as being sensitive
- Risk of legal noncompliance if information is used for another purpose or disclosed without authority
- Risk of privacy complaints if there is legal noncompliance or the public is surprised by a use for another purpose or a disclosure
- The most commonly stolen IP is customer databases

REDUCING THE RISK

- Block USB ports to reduce data loss
- Monitoring emails that employees send to ensure data remains secure
- Force change of password regularly
- Educate staff on not sharing passwords
- User access reviews to ensure password
- Ensure data protection / data destruction policies are followed
- Effective due diligence: KYC/KYE/KYS/KYSS

CASE STUDY

- Wikileaks – published tens of thousands of classified military documents
- Industrial espionage – stealing trade secrets and designs etc.
- Facebook has hundreds of millions of users and sensitivities of data loss
- Kim Dotcom – piracy of documents via Megaupload
- Aaron Schwartz – indicted for computer fraud and downloading documents from JSTOR with the intention to share on web..



The Future of GRC

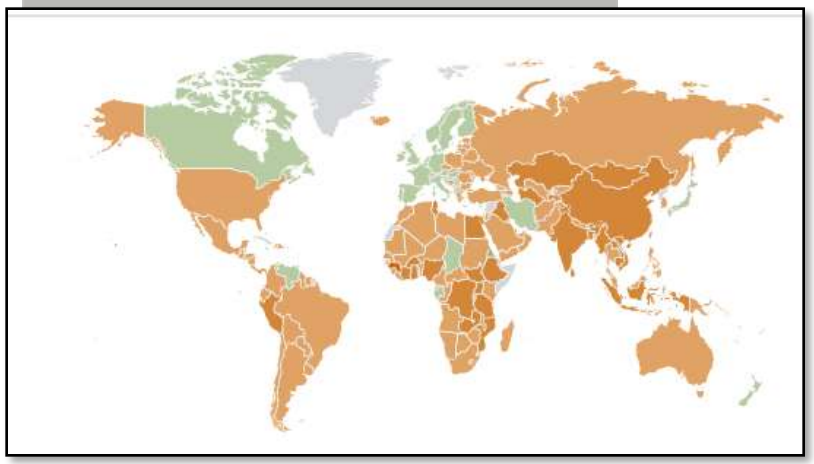
Delivering ROI in time of increased risk:

The New KYC Paradigm & GRC Technology

Due diligence dynamics evolving

It's no longer all about 'KYC'

Real GDP Growth
IMF Data Mapper (September 2011)



Countries that attract the greatest investment carry the greatest risk

Transparency International
Corruption Perceptions Index (December 2012)

Regulatory Drivers

- Anti-money laundering
- Anti-Bribery & corruption
- Financial services standards

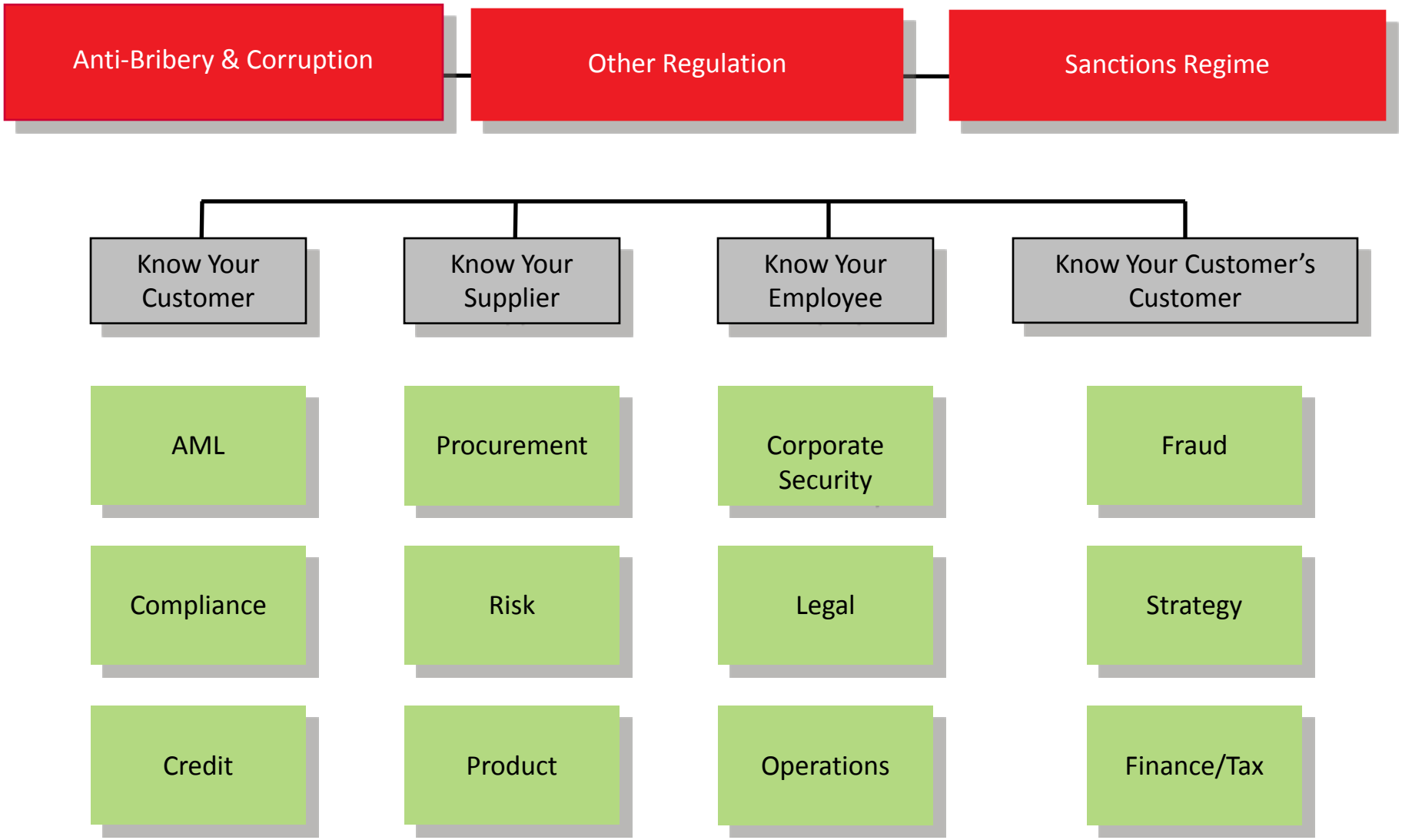
Business Drivers

- Emerging market investment
- Business reputation management
- Ethical codes and standards
- Avoiding fines and penalties
- Ongoing business process efficiency

13

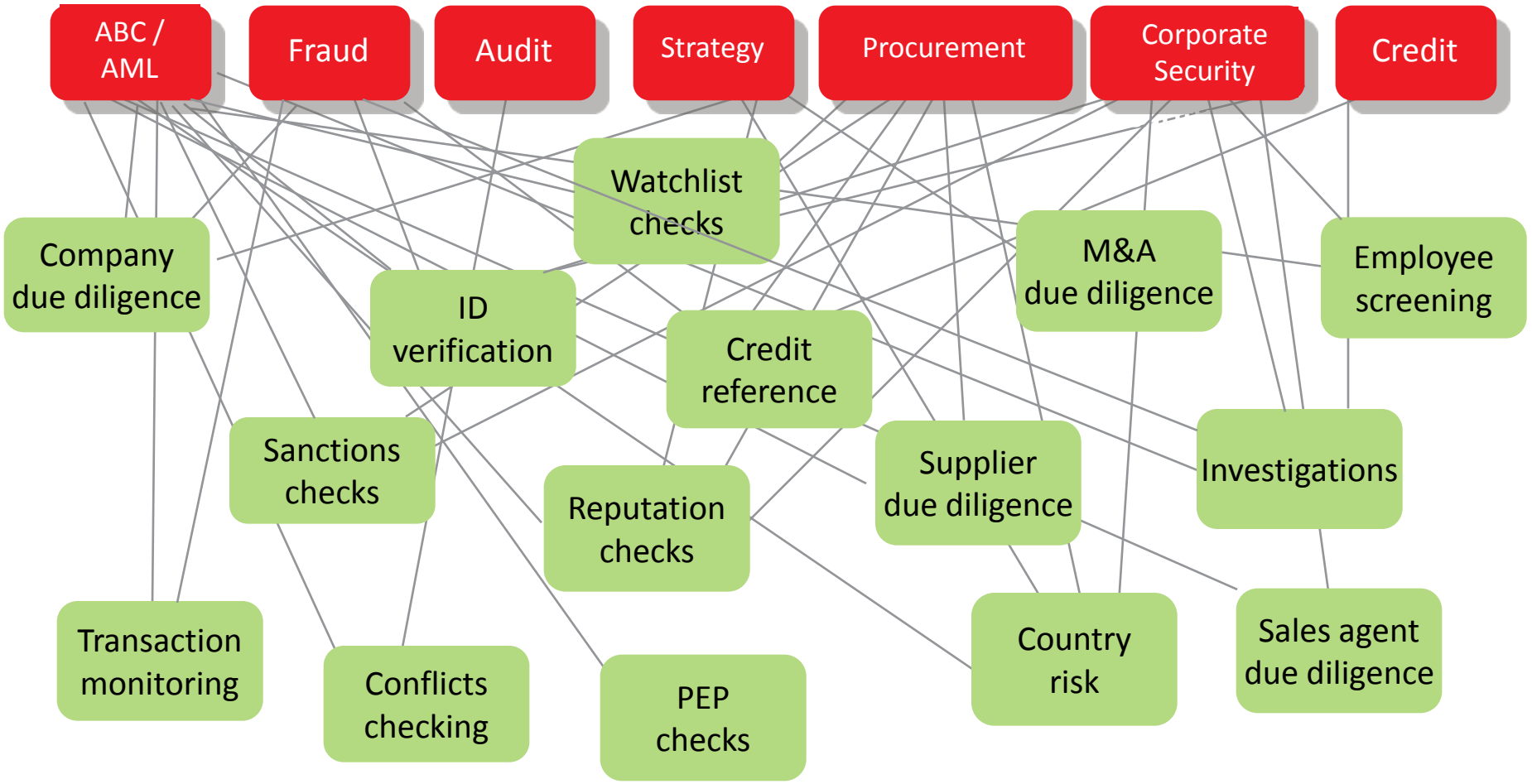
Due diligence dynamics evolving

It's no longer all about 'KYC'



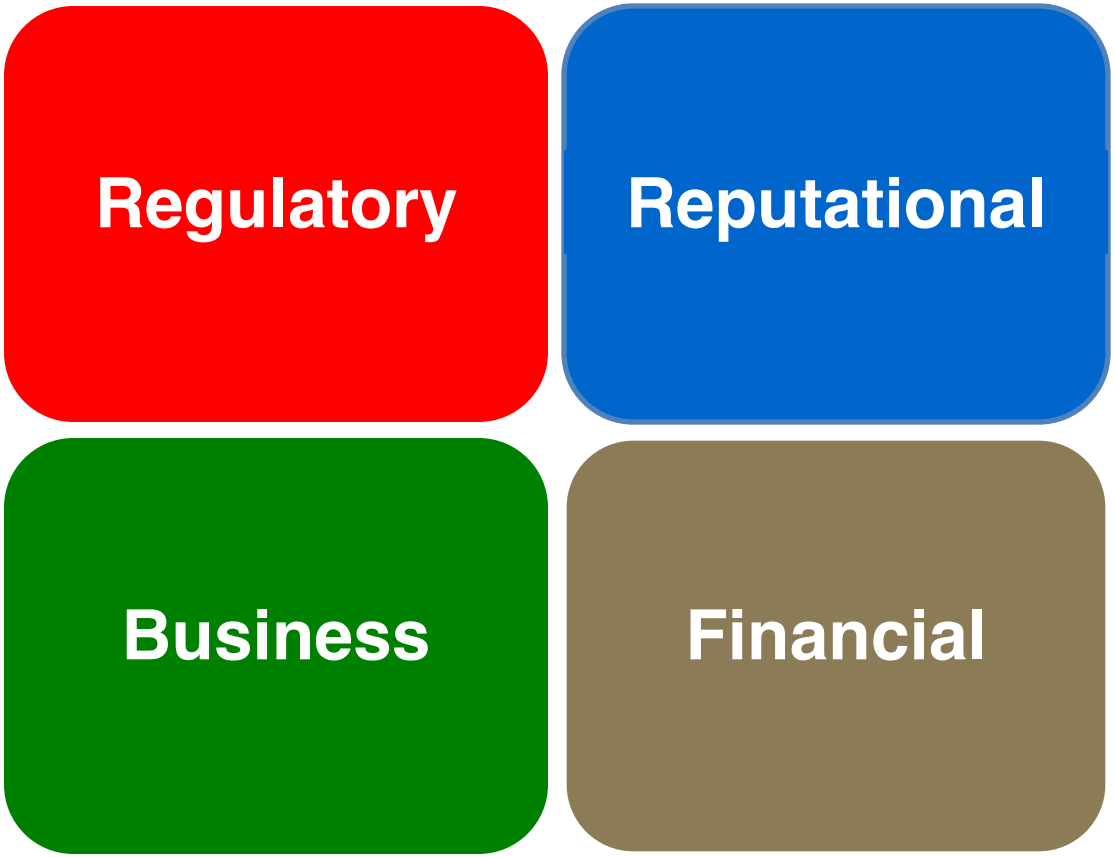
Due diligence dynamics evolving

It's no longer all about 'KYC'



Towards a consistent due diligence process

Benefits of consolidating key due diligence tasks



Towards a consistent due diligence process

Benefits of consolidating key due diligence tasks

Regulatory

- Helps demonstrate robust ABC and sanctions compliance and adherence to associated industry standards & best practice
- Helps implementation and ongoing maintenance of a consistent risk-based approach scaled to company size
- Enables indication of clear risk flags and maintenance of comprehensive audit trail
- Enables more discipline and control to be implemented through hard coded role profiles, permission settings, incident escalation and approvals to support ‘four eyes’ check

Towards a consistent due diligence process

Benefits of consolidating key due diligence tasks

Reputational

- Helps protect hard earned brand and business reputations through comprehensive and consistent due diligence process to mitigate AML, ABC and other risks
- Helps business maintain strong ethical standards and adhere to codes of conduct
- Helps demonstrate and promote robust processes and controls to customers and business partners

Towards a consistent due diligence process

Benefits of consolidating key due diligence tasks

Business

- Effective and consistent due diligence process improves speed of execution and competitive edge in key high risk developing markets
- Efficient and streamlined onboarding experience enhances both external and internal customer and other third-party service levels
- Helps Compliance and associated teams reinforce benefits and emphasise positive contribution to business success through improved service levels and provision of more effective management intelligence to support Board engagement

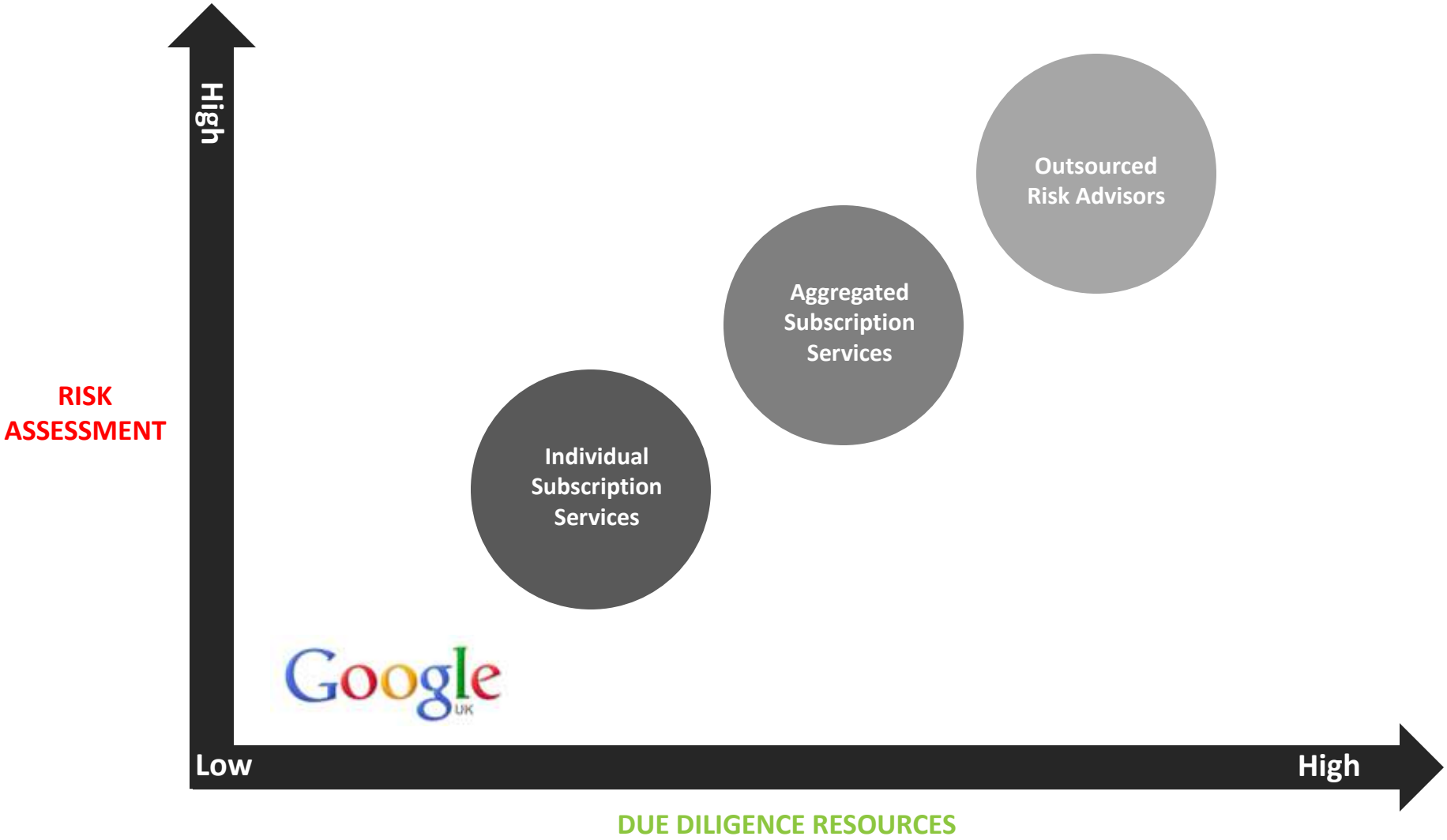
Towards a consistent due diligence process

Benefits of consolidating key due diligence tasks

Financial

- Helps mitigate regulatory fines, financial penalties and contract debarment
- Prompts regular review and audit of due diligence research resources to address content overlap and cost duplication thereby reducing cost of sale etc
- Consistent process enables business to easier test and benchmark cost efficiencies and other associated benefits

Emerging GRC Solutions & Tools



Questions