Leveraging Internal Audit in Fraud Risk Management

CA (Dr) K. Paul Jayakar

M.Com., FCA, PhD, DIRM, CRISC, FoIA

November 16th, 2024

Session Outline

1. Internal Audit

2. Data Security

3. Data Privacy

4. Fraud Risk

5. Conclusion

Session Outline

We will cover these skills

- Internal Audit Techniques
- Privacy And Protection Laws
- Fraud Risk Detection Methods

First Skill – IA techniques

1. **Risk Assessment and Prioritization**
2. **Process and Control Mapping**
3. **Sampling and Testing**
4. **Data Analytics**
5. **Interviews and Questionnaires**
6. **Walkthroughs and Observations**
7. **Document and Policy Reviews**
8. **Control Self-Assessment (CSA)**
9. **Benchmarking**
10. **Continuous Auditing and Monitoring**
11. **Forensic and Investigative Techniques**

WHAT ARE FEATURES TO CONSIDER FOR INTERNAL AUDIT TOOLS?

User-Friendly Interface

CAPA Features

Options for Creating Reports

Scheduling

Cloud-Based Options

aloa

First Skill – IA techniques …

1. **Enterprise Risk Management (ERM) – COSO -**for integrating risk management with strategic planning.

2. **ISO 31000 -** principles and guidelines for risk management across any organization

3. **NIST Risk Management Framework (RMF) -** used in cybersecurity,

4. **COBIT (Control Objectives for Information and Related Technologies) -** IT management and governance framework

5. **FAIR (Factor Analysis of Information Risk) -** quantitative risk framework focusing specifically on cybersecurity and operational risk

First Skill – IA techniques …

6. **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) -** emphasizes self-directed assessment

7. **M_o_R (Management of Risk) -** UK government - risk across strategic, project, and operational levels

8. **Basel III -** risk management related to capital requirements, stress testing, and liquidity in banks

9. **ITIL (Information Technology Infrastructure Library) Risk Management** - guidelines for managing IT service-related risks, focusing on aligning IT services with the needs of the business.

10. **PMBOK (Project Management Body of Knowledge) Risk Management -** specifically for project management

11. **CRISC (Certified in Risk and Information Systems Control -** risk management certification and framework for IT (NIST)

Second Skill - Privacy And Data Protection Laws

Laws - Society

An instrument which regulates human conduct/behavior. Law means Justice, Morality, Reason, Order, and Righteous from the view point of the society

Laws - Legislature

Law means Statutes, Acts, Rules, Regulations, Orders, and Ordinances from point of view of legislature.

Circulars, policies

Policies are like rules.

Circulars are for updates and reminders.

Second Skill –- Privacy And Data Protection Laws ...

1. **India**: The ***Digital Personal Data Protection Act*** (DPDP), 2023, regulates personal data protection, emphasizing user consent, data minimization, and data storage restrictions and the ***Information Technology Rules*** (IT Act) (2011 and 2021 amendments) – India provide sectoral data protection laws.

2. **European Union**: The ***General Data Protection Regulation*** (GDPR), effective since 2018, is one of the most stringent data protection laws, influencing many global privacy laws.

3. **United States**: While there is no federal law, multiple states have enacted their own data privacy laws:

   A. **California**: The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) set comprehensive rights and protections for consumer data.

   B. **Virginia, Colorado, and Utah**: Each state has similar laws (VCDPA, CPA, and UCPA, respectively), providing consumer rights and business obligations.

   C. **Ohio and Wisconsin**: Ohio's Personal Privacy Act and Wisconsin's proposed data protection bill offer guidelines on data rights and protections.

Second Skill –- Privacy And Data Protection Laws …

4. **China**: The Personal Information Protection Law (PIPL) and Data Security Law (DSL) regulate personal data collection, processing, and cross-border transfers with a strong focus on national security.

5. **Brazil**: The Lei Geral de Proteção de Dados (LGPD) is Brazil's comprehensive data protection law, largely modeled on the GDPR.

6. **South Africa**: The Protection of Personal Information Act (POPIA) sets data privacy standards for collecting and processing personal information.

7. **Canada**: The Personal Information Protection and Electronic Documents Act (PIPEDA) governs data privacy across most private-sector organizations, with some provinces having additional laws.

8. **Australia**: The Privacy Act 1988, along with the Australian Privacy Principles, regulates personal data in various sectors.

9. **South Korea**: The Personal Information Protection Act (PIPA) provides robust data privacy regulations and has been regularly updated to strengthen privacy protections.

Second Skill –- Privacy And Data Protection Laws …

10. **Japan**: The Act on the Protection of Personal Information (APPI) applies to both domestic and international companies handling Japanese citizens' data.

11. **New Zealand**: The Privacy Act 2020 emphasizes consumer rights, data collection limitations, and data breach notifications.

12. **Convention 108+ - Council of Europe**

    A.   The only binding international treaty on data protection, which has been modernized as Convention 108+, extends GDPR-like rights to Council of Europe member states and signatories.

13. **Other regions** with comprehensive privacy laws include the UAE, Israel, Singapore, and many Latin American and African countries, as they adapt to a global emphasis on privacy and data protection

India, SAFTA & The Eurasian Economic Union

Second Skill –- Privacy And Data Protection Laws …

1. https://www.dlapiperdataprotection.com/

Third Skill -Fraud Risk Detection Methods

- Fraud represents a significant problem for governments and businesses and specialized analysis techniques for discovering fraud using them are required.

- Some of these methods include knowledge discovery in databases, data mining, machine learning and statistics

Third Skill - Fraud Risk Detection Methods

The set of activities aimed at identifying, assessing, and mitigating risks related to fraudulent activities within an organization.

A. **Risk Assessment**: Identify potential fraud risks.
B. **Internal Controls**: Establish safeguards to mitigate fraud risks.
C. **Monitoring & Detection**: Ongoing oversight of fraud prevention measures.
D. **Response Strategy**: Actions to take when fraud is detected

Third Skill - Fraud Risk Detection Methods

IT Systems as a Control Mechanism:

1. Automation of internal controls to prevent fraudulent activities.

2. Use of real-time monitoring and data analysis to detect suspicious transactions.

3. Integration with Fraud Risk Management:

4. IT systems help implement fraud detection software, segregation of duties, and data security protocols.

- Example:

- A financial institution uses an IT system to monitor all transactions in real-time and flag those that deviate from normal behaviour patterns, such as large withdrawals from an unusual location.

Third Skill - Fraud Risk Detection Methods

Key Areas of IT Systems Audit in Fraud Risk Management

- **Access Controls**:
1. Review the effectiveness of **user authentication** systems (password policies, multi-factor authentication).
2. Evaluate **role-based access controls** to ensure only authorized users can access sensitive data.

- **Data Encryption**:
1. Ensure that data (both **in transit and at rest**) is encrypted to prevent unauthorized interception or modification.

- **Log Management & Monitoring**:
1. Assess how well IT systems **track user activities** and generate audit logs to detect unauthorized access.

- **Network Security**:
1. Evaluate firewalls, intrusion detection systems, and anti-malware defences to ensure that they protect the system from external threats.

Third Skill - Fraud Risk Detection Methods

Data Security and Its Role in Preventing Fraud

- <u>Importance of Data Security in Fraud Prevention</u>:

  > Data security ensures that sensitive information (financial records, customer data, etc.) is protected from cyberattacks, preventing fraud.

- Common Data Security Measures:

  Encryption: Ensure all sensitive data is encrypted.

  Data Backup: Regular backups to recover from ransomware or data loss.

  Endpoint Security: Protect devices like laptops, mobile phones, and workstations that access company systems.

Third Skill - Fraud Risk Detection Methods

Key Audit Procedures for IT Systems in Fraud Risk Management

1. **Risk Assessment**:

   Identify critical IT systems that manage financial data, transactions, or customer records.

2. **Testing of Controls**:

   Test the effectiveness of controls such as access controls, encryption, and user activity monitoring.

3. **System Vulnerability Scans**:

   Conduct regular scans for system vulnerabilities, outdated software, or weak security protocols.

4. **Review of Incident Response Plan**:

   Ensure that the organization has a documented incident response plan to handle data breaches or system failures.

Third Skill - Fraud Risk Examples

1. Expense Reimbursement Fraud Detection

- **Case**: An employee was submitting inflated travel and meal expenses.
- **Detection**: Internal auditors used data analytics to review expenses across employees and found recurring patterns of inflated claims from a single employee.
- **Outcome**: The organization established stricter controls for verifying expense receipts and imposed disciplinary actions.

Third Skill - Fraud Risk Examples

2. Procurement and Vendor Collusion

▪ **Case**: A procurement manager was colluding with an external vendor, awarding contracts in exchange for kickbacks.

▪ **Detection**: Auditors analyzed procurement transactions and identified repeated awards to the same vendor without competitive bidding. They also identified a connection between the vendor and the procurement manager.

▪ **Outcome**: The procurement process was revamped with stronger controls for vendor selection and independent reviews, and the employee was terminated.

Third Skill - Fraud Risk Examples

3. Fictitious Employee Payroll Fraud

- **Case**: Payroll fraud occurred when a manager added fictitious employees to the payroll and pocketed their salaries.

- **Detection**: Internal audit reviewed payroll records, matching employee data with HR records and physical attendance. They discovered several employees on payroll with no physical records or actual assignments.

- **Outcome**: Fraudulent records were purged, the manager was dismissed, and additional payroll checks were implemented.

Third Skill - Fraud Risk Examples

4. Credit Card Fraud

- **Case**: Corporate credit card misuse by employees for personal expenses disguised as business costs.

- **Detection**: Internal auditors used data mining and transaction monitoring to identify unusual patterns, such as high-value personal purchases during off-business hours or weekends.

- **Outcome**: Policies for corporate card usage were tightened, and certain employees were disciplined.

Third Skill - Fraud Risk Examples

5. Financial Statement Manipulation

- **Case**: Management manipulated financial statements to meet revenue targets.

- **Detection**: The internal audit team conducted forensic analyses on the revenue recognition process and identified discrepancies between sales records and cash receipts.

- **Outcome**: The manipulation was disclosed to the board, which resulted in restating financials and revising internal controls for financial reporting.

Third Skill - Fraud Risk Examples

6. Inventory Theft and Misappropriation

- **Case**: Employees were stealing inventory items from warehouses and disguising it as operational losses.

- **Detection**: Internal auditors implemented surprise inventory counts and matched records with sales data. This revealed inventory discrepancies and unauthorized access to warehouses.

- **Outcome**: Losses were reduced by implementing stricter access controls and conducting regular inventory audits.

Third Skill - Fraud Risk Examples

7. Information Technology (IT) Fraud

- **Case**: An IT employee granted unauthorized access to systems in exchange for bribes.

- **Detection**: Auditors identified unusual access logs and noticed certain systems were accessed during off-hours by unauthorized users.

- **Outcome**: The employee was dismissed, access policies were strengthened, and a system alert was introduced for unauthorized access attempts.

Third Skill - Fraud Risk Examples

8. Overbilling and False Invoicing

- **Case**: A contractor submitted invoices for services that were either not delivered or inflated.

- **Detection**: Internal audit compared invoices to the actual work completed and identified discrepancies. They also performed vendor background checks and discovered a link between the contractor and an employee.

- **Outcome**: The contractor relationship was terminated, and enhanced invoice verification processes were put in place.

Third Skill - Fraud Risk Examples

9. Financial Fraud in Revenue Recognition

- **Case**: Sales employees recorded false sales at the end of the financial period to meet targets.

- **Detection**: Auditors reviewed end-of-quarter sales transactions and found that goods were recorded as sold without shipping confirmations or valid customer orders.

- **Outcome**: Sales targets were re-evaluated, and the sales team was trained on proper revenue recognition policies.

Third Skill - Fraud Risk Examples

10. Conflict of Interest Fraud

- **Case**: An employee awarded contracts to a company owned by a relative.

- **Detection**: During an audit, the team noticed unusual vendor selection patterns and discovered that the awarded company had links to the employee's family.

- **Outcome**: The employee faced disciplinary actions, and a conflict-of-interest disclosure process was implemented across the company.

Third Skill - Fraud Risk Examples

11. Ghost Billing in Medical and Healthcare

- **Case**: A healthcare organization discovered that some doctors were billing for services never rendered (e.g., ghost patients).

- **Detection**: Internal auditors conducted a random sampling of patient records and found inconsistencies between services billed and patient appointment records.

- **Outcome**: Billing practices were revised, disciplinary action was taken against implicated personnel, and real-time patient record audits were implemented.

Third Skill - Fraud Risk Examples

12. Fraudulent Insurance Claims

- **Case**: Employees at an insurance company processed false claims by creating fictitious client accounts.

- **Detection**: Internal auditors used data analytics to detect unusual claim patterns and identified accounts with suspiciously high claims with no detailed records.

- **Outcome**: Claims procedures were tightened, and random audits on claim approvals were introduced.

Third Skill - Fraud Risk Examples

13. Cybersecurity and Data Manipulation Fraud

- **Case**: An employee manipulated customer data for personal gain, affecting service outcomes.

- **Detection**: Audit logs were reviewed by internal audit, who identified unauthorized changes to sensitive data.

- **Outcome**: The employee was terminated, data modification protocols were strengthened, and additional monitoring was put in place for sensitive systems.

Third Skill - Fraud Risk Detection Methods

1. **Phishing**
2. **Data breach**
3. **Denial of service**
4. **Ransomware**
5. **Identity theft**
6. **Friendly fraud**
7. **Card testing fraud**
8. **Insider threats**
9. **Viruses**

Third Skill - Fraud Risk Detection Methods

Information Retrieval (IR)
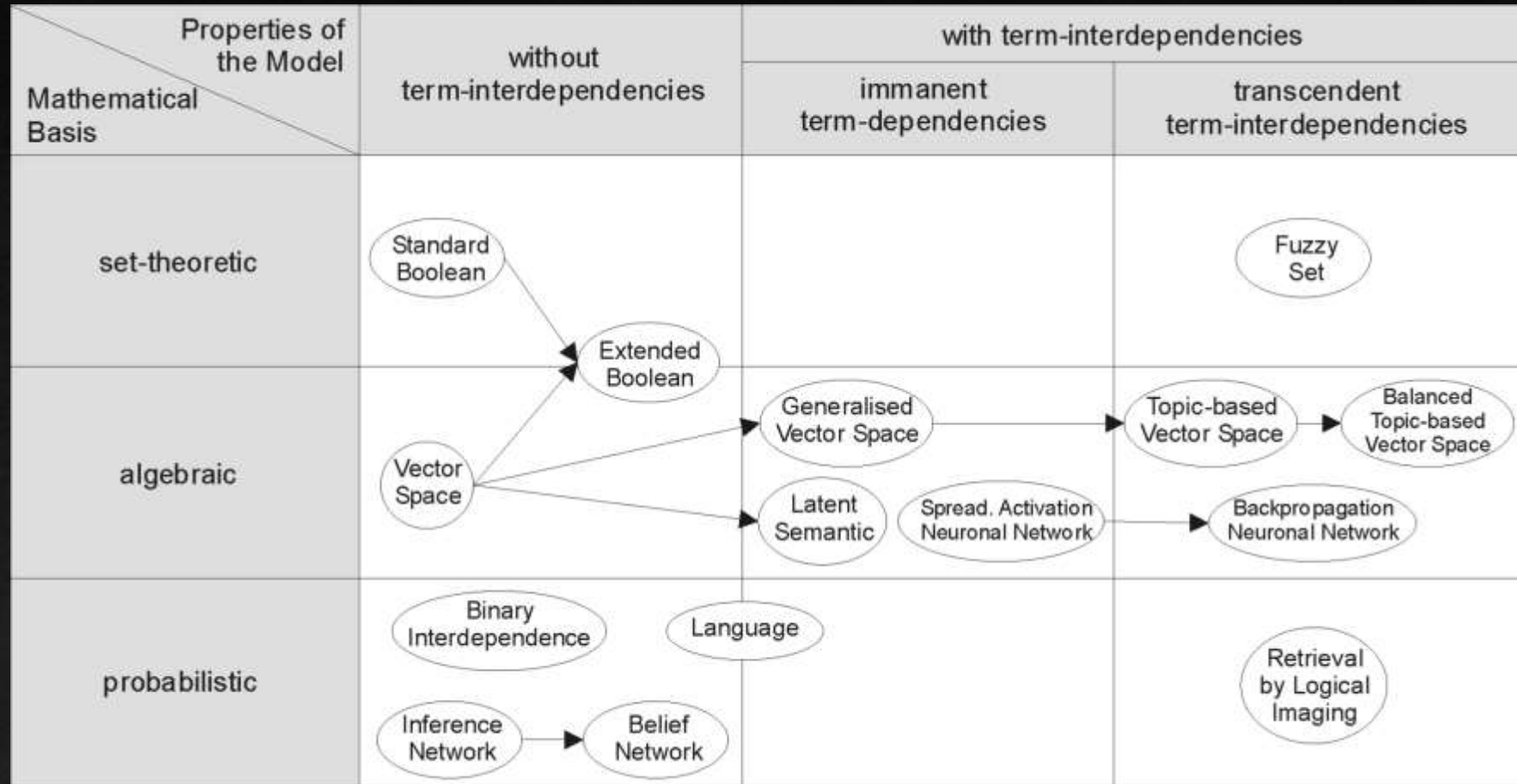
Third Skill – Fraud Risk Detection Methods
IR – *General applications*

- **Digital libraries**
- **Information filtering**
  - Recommender systems
- **Media search**
  - Blog search
  - Image retrieval
  - 3D retrieval
  - Music retrieval
  - News search
  - Speech retrieval
  - Video retrieval

- **Search engines**
  - Site search
  - Desktop search
  - Enterprise search
  - Federated search
  - Mobile search
  - Social search
  - Web search

Third Skill - Fraud Risk Detection Methods
IR - *Domain-specific applications*

- Expert search finding

- Genomic information retrieval

- Geographic information retrieval

- Information retrieval for chemical structures

- Information retrieval in software engineering

- Legal information retrieval

- Vertical search

Third Skill - Fraud Risk Detection Methods
IR - *Other retrieval methods*

- Adversarial information retrieval

- Automatic summarization

- Multi-document summarization

- Compound term processing

- Cross-lingual retrieval

- Document classification

- Spam filtering

- Question answering

TYPES OF FRAUD DETECTION TECHNIQUES

Statistical data analysis
- Statistical parameter calculation
- Probability distribution & models
- Regression analysis
- Data matching

Artificial intelligence
- Data mining
- Neural networks
- Machine learning
  - Supervised learning
  - Unsupervised learning
- Pattern recognition

TOOLBOX

Hierarchic Layout

Orthogonal Layout

https://live.yworks.com/demos/showcase/frauddetection/

DEMO
https://live.yworks.com/demos/showcase/frauddetection/
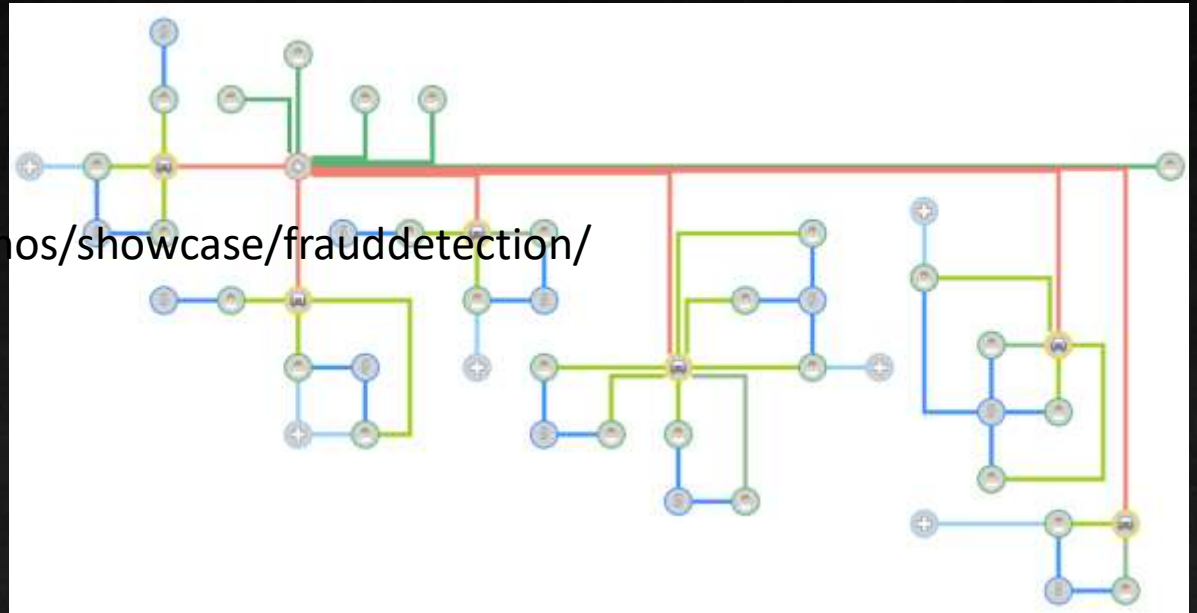
Third Skill - Fraud Risk Detection Methods

- **Website**

- https://www.yworks.com/pages/fraud-detection-through-visualization

- **Demo**

- https://live.yworks.com/demos/showcase/frauddetection/
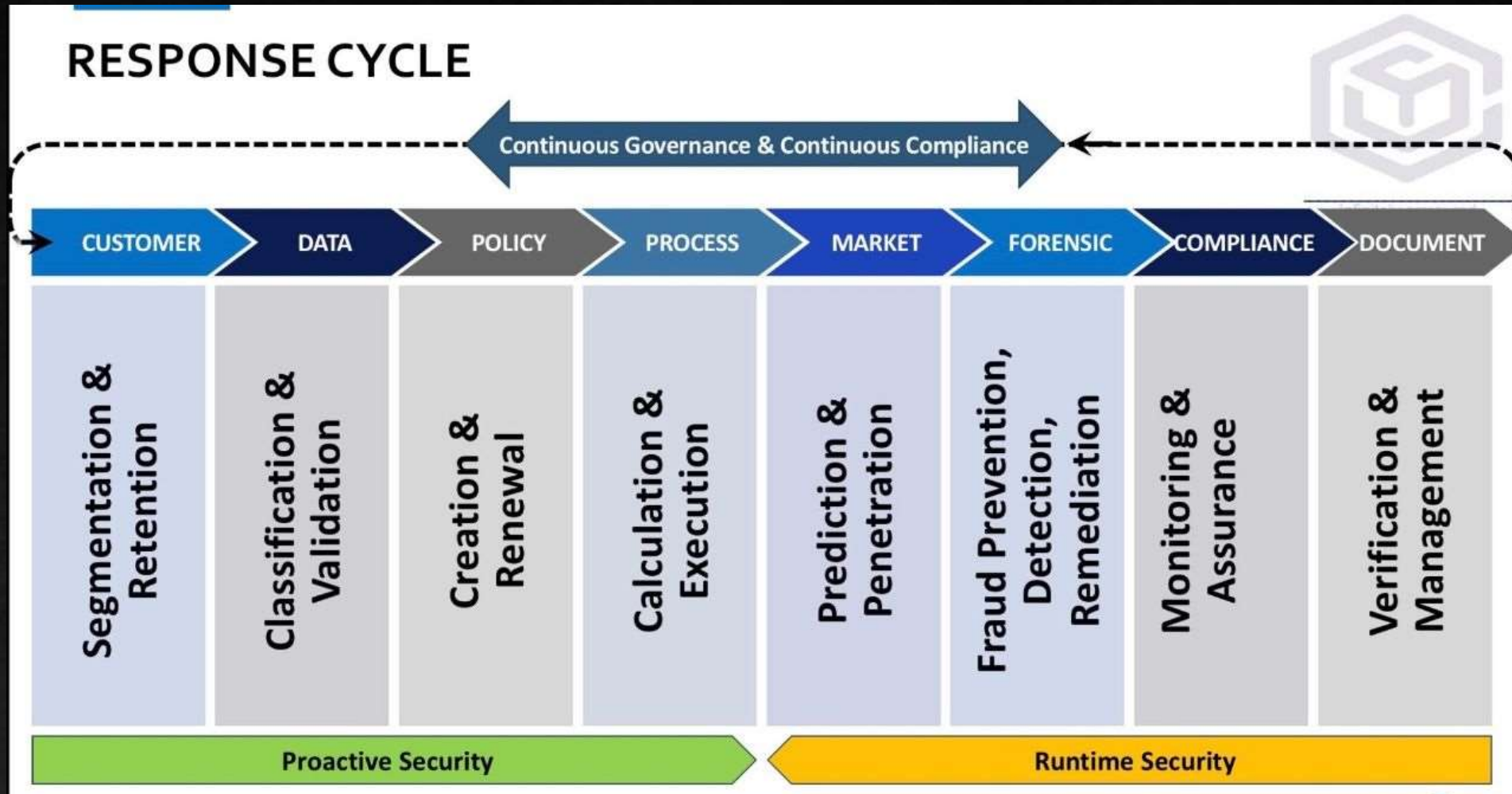
Third Skill - Fraud Risk Detection Methods

Third Skill - Fraud Risk Detection Methods

- Risk assessment tools and techniques by Tony Ridley

- https://www.researchgate.net/publication/377207094_Risk_Assessment_Techniques_Strengths_Weaknesses_Compared

First Lesson Summary

Here is what we learned

First skill:
Internal Audit Techniques

Second skill:
Privacy And Protection Laws

Third skill:
Fraud Risk Detection Methods

Thank You

pauljayakar@gmail.com