Staying Ahead of Risk

ID4AFRICA2019

June 2019

Presented by:
Rakesh Kaul
Government & Public Sector Leader
PwC India
Technology is helping solve some of the largest societal problems at scale for the people.
...and Identity is the foundation for the “Digital Nation” construct..

Seeding in other Functional ID systems

Single Source of Identity Trust - Foundational ID

PwC
... and this Identity Ecosystem needs to be reliable and resilient..

Critical challenges in implementation of National IDs

1. Gaps in Legal and institutional environment such as absence of personal data protection
2. Privacy of Personal Sensitive Information and Security related risks
3. Complicated Enrolment process and the cost associated with getting one enrolled in the National ID program
4. Scarcity of Infrastructure and associated challenges
5. Sustainability of the Program
To make it reliable and resilient, managing risk becomes paramount.

National ID program discontinued due to privacy concerns

Vulnerability in ID cards due to security flaw

Personal Information stolen from National ID Database

Note: Information regarding the ID programs is based on public information available on the respective newspaper websites.
To make it reliable and resilient, managing risk becomes paramount.

Staying Ahead of Risk..

GRC Framework

Staying ahead of risks

Governance

- Governance Framework
- Organization Skill and Capability
- Adoption of the right Framework

Compliance

- Periodic Assessment
- 24*7 Continuous Monitoring
- Forensics

Risk

Note: Information regarding the ID programs is based on public information available on the respective newspaper websites.
## Risk Management - Identify Risks

### Objective
- Identify risks
- Assess risks
- Determine risk response

### How

<table>
<thead>
<tr>
<th></th>
<th>Identify risks</th>
<th>Assess risks</th>
<th>Determine risk response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Consider the organizational goals &amp; business drivers of NID</td>
<td>Key highlights</td>
<td>Leveraging Information Security Forum and knowledge repositories</td>
</tr>
<tr>
<td>2</td>
<td>Scan the internal &amp; external environment and assets of NID</td>
<td>Early deployment of Risk Simulation and Fraud Analytics to analyse the past incident data and simulate risks</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Inventory Threat Landscape</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Historical &amp; forward-looking analyses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Inventory key risks that should be assessed and monitored</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### External Threats
- Regulatory Landscape
- Internal Threats

### Risk Register

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Category</th>
<th>Risk Impact</th>
<th>Likelihood</th>
<th>Risk Rating</th>
<th>Score</th>
<th>Neutral Risk Tolerance</th>
<th>Neutral Risk Rating</th>
<th>Neutral Risk Action</th>
</tr>
</thead>
</table>

**Key highlights**

- Leveraging Information Security Forum and knowledge repositories
- Early deployment of Risk Simulation and Fraud Analytics to analyse the past incident data and simulate risks
## Risk Management - Assess Risks

### Objective
- Identify risks
- Assess risks
- Determine risk response

### How

<table>
<thead>
<tr>
<th>Risk Classification</th>
<th>Objective</th>
<th>Identify risks</th>
<th>Assess risks</th>
<th>Determine risk response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>Reputation, Legal/Regulatory</td>
<td>Likely</td>
<td>Occasional</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Earnings, Solvency, Ratings</td>
<td>Minor</td>
<td>Moderate</td>
<td>Adverse</td>
<td>Significant</td>
</tr>
</tbody>
</table>

### Risk Scenarios
- **Identify the interrelationships and concentrations of risk**
- **Develop risk rating scales that consider cross-organizational impact**
- **Develop a heat map or radar of key risks**
- **Update risk appetite and tolerances**

### Risk Scenarios

#### Heat Map
- Likelihood, impact & correlation using simulations / scenario analyses
- Identify the interrelationships and concentrations of risk
- Develop risk rating scales that consider cross-organizational impact
- Develop a heat map or radar of key risks
- Update risk appetite and tolerances
## Risk Management - Determine Risk Response

<table>
<thead>
<tr>
<th>Objective</th>
<th>Identify risks</th>
<th>Assess risks</th>
<th>Determine risk response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How</strong></td>
<td>Conduct a series of workshops to validate risks</td>
<td>Assess control effectiveness in remediation of associated risks to meet risk appetite</td>
<td><strong>1</strong> Identify and design Controls</td>
</tr>
<tr>
<td></td>
<td>Map approved controls to identified risks</td>
<td>Prioritize risk remediation activities to align with reasonable and expected investment</td>
<td><strong>2</strong> Implement Controls</td>
</tr>
<tr>
<td></td>
<td>Identify Risks</td>
<td>Assess Controls</td>
<td><strong>3</strong> Assess and Test Controls</td>
</tr>
<tr>
<td></td>
<td>Map Controls to Risks</td>
<td>Prioritize Remediation</td>
<td><strong>4</strong> On-going Risk Monitoring</td>
</tr>
</tbody>
</table>

PwC
In order to effectively mitigate and respond to the Risks it is essential to have a robust Governance in place...

**Governance**

**Vision & Strategy**
- Discuss and agree GRC vision
- Align GRC vision with the objective
- Identify applicable regulations and standards
- Identify applicable compliance requirements
- Review and update policy and procedures with respect to information security and privacy

**Org. Structure, Roles & Responsibility**
- Identify and define GRC organization structure
- Define the Role and Key Performance Indicators (KPIs) for the individuals
- Institutionalized GRC by proposing various groups:
  - Executive Committee
  - Working group

**Reporting & Dashboarding**
- Define reporting requirements
  - Type
  - Frequency
  - Mechanism
- Discuss and define communication strategy
- Define integrated Dashboard for various levels
  - Senior Management
  - Operation team
..and regular Compliance checks through continuous monitoring and periodic assessment

- Monitoring
  - Incident Identification
  - Incident Classification
  - Real Time Device Monitoring
  - Vulnerability & Penetration Testing
  - Security Intelligence

- Advising
  - Incident Notification
  - Awareness & Technology
  - Countermeasures Selection

- Managing
  - Incident Response
  - Incident Recovery
  - Tracking and Tracing

---

**Business Requirement**
- 24*7 Continuous monitoring

**Laws and Regulations**
- Planning
  - Audit Charter
  - Understand sub process, controls and risk
  - Prepare work program

- Field Work
  - Process walk through
  - Conduct testing (walkthrough, observations, enquiries etc)
  - Identify gaps

- Report and closure
  - Prepare draft report - (observations, risk rating etc)
  - Agree and closure

**Contractual Requirement**
- Evidence Extraction and Storage (Acquisition)
  - Appropriate clearances
  - Appropriate chain of custody log
  - Time record

- Review and Analysis
  - Backup of the "original"
  - Time-zone checks
  - Perform testing

- Investigation Completion and Engagement Wrap-up

---

**Privacy**
- Accuracy
  - Monitoring
    - Incident Identification
    - Incident Classification
    - Real Time Device Monitoring
    - Vulnerability & Penetration Testing
    - Security Intelligence

---

**People**
- Technology
- Processes
- Policy

PwC
“It is not the strongest of the species that survives, nor the most intelligent, but the most responsive to change.”

–Charles Darwin

Thank You
Benefits of GRC Program

Key risks

- Insiders and ecosystem partner’s threats
- Intrinsic vulnerabilities associated with technology such as zero day attacks
- Process vulnerable to fraud
- Changing risk landscape
- Targeted attacks on ID entity
- SLA breaches

Benefits

Management of existing and emerging risks
- Early identification of threats for prosecution

Governance
- Actionable, real time reporting to ID Entity
- Ensure closed looping

Compliance
- Processes aligned to risks
- Consistent compliance across entire ecosystem

Risk culture
- Risk ownership and accountability
- Culture of ethics and compliance

Performance
- Timely prioritized reporting
- Support RCA for breaches