Staying Ahead of Risk

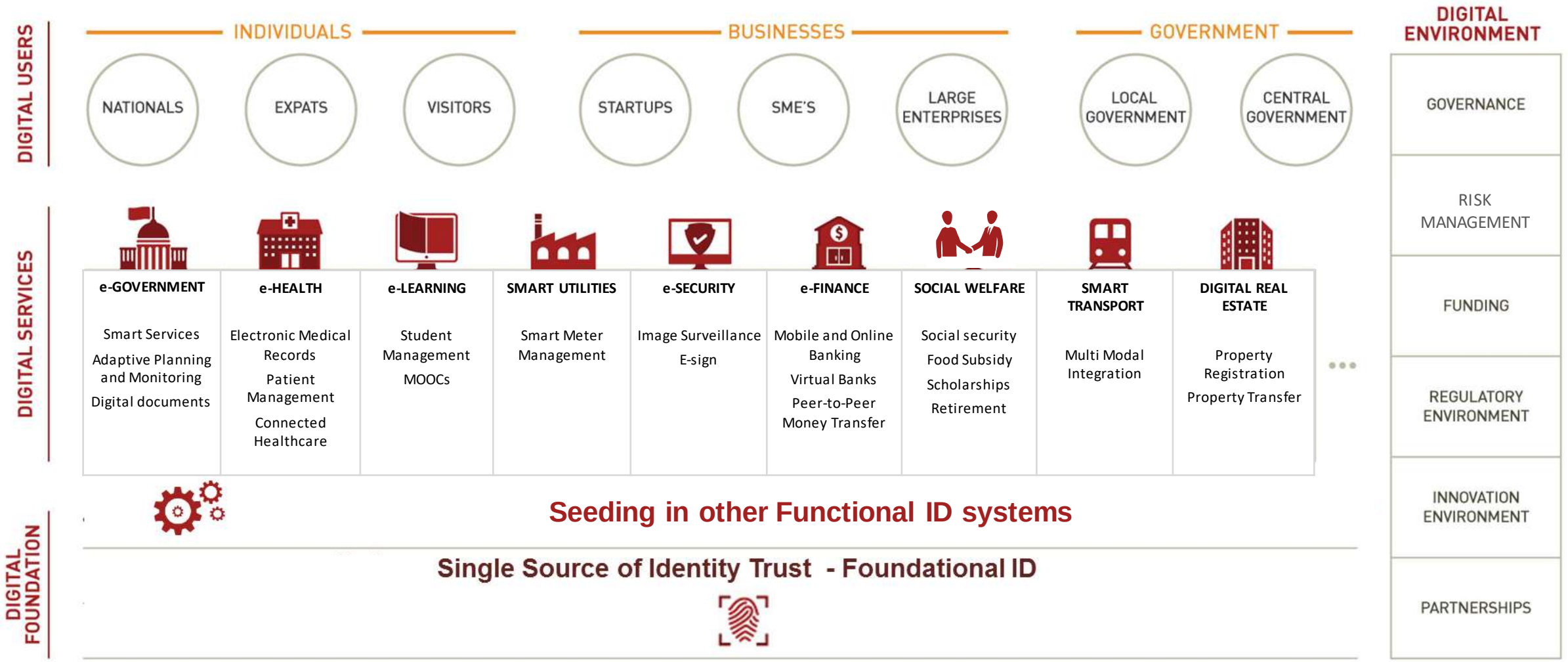
ID4AFRICA2019

June 2019

Presented by:
Rakesh Kaul
Government & Public Sector Leader
PwC India

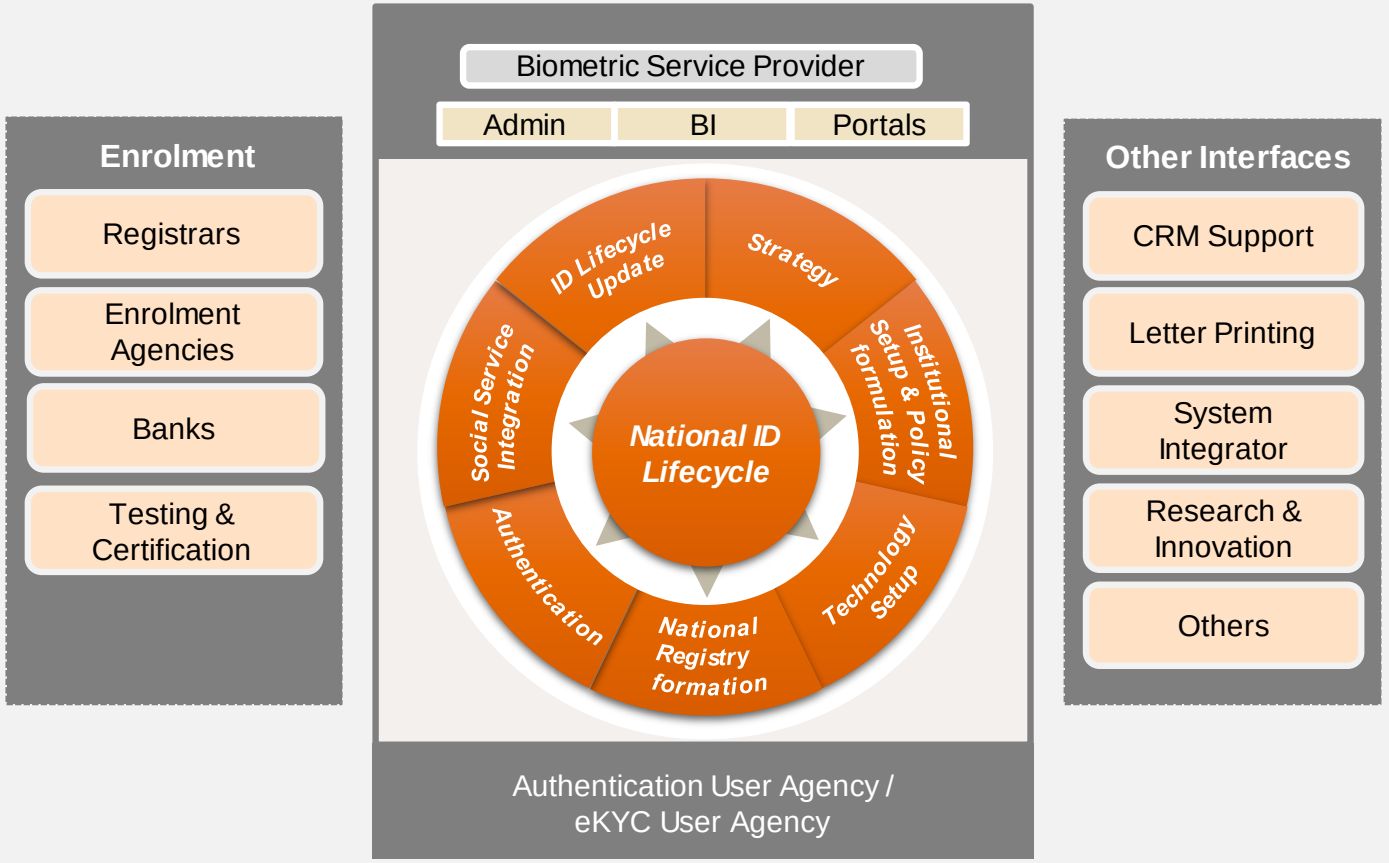
Technology is helping solve some of the largest societal problems at scale for the people..

...and Identity is the foundation for the "Digital Nation" construct ..



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

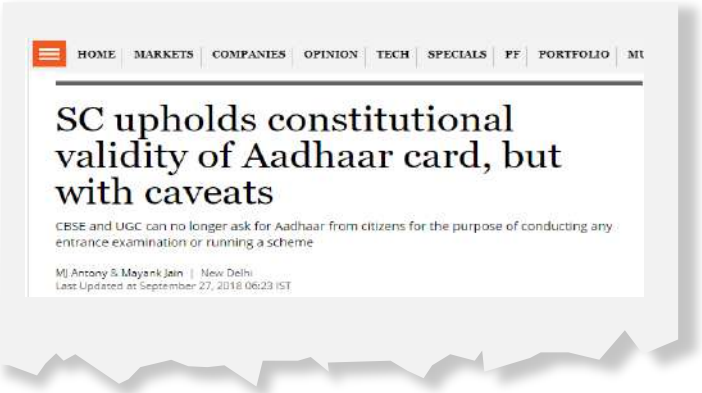
Identity Ecosystem



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..


HOME | MARKETS | COMPANIES | OPINION | TECH | SPECIALS | PF | PORTFOLIO | MU

SC upholds constitutional validity of Aadhaar card, but with caveats

CBSE and UGC can no longer ask for Aadhaar from citizens for the purpose of conducting any entrance examination or running a scheme

MJ Antony & Mayank Jain | New Delhi
Last Updated at September 27, 2018 06:23 IST

Vulnerability in ID cards due to security flaw


BBC Sign in News Sport Weather Shop Reel Travel More

NEWS

Home Video World Asia UK Business Tech Science Stories Entertainment &

Technology

Security flaw forces Estonia ID 'lockdown'

3 November 2017 Share

National ID program discontinued due to privacy concerns


the japan times

NEWS

Theft of data belonging to millions of South Koreans forces ID system overhaul

AP

SEOUL - After an avalanche of data breaches, South Korea's national identity card system has been raided thoroughly by hackers that the government says it might have to issue new ID numbers to every citizen c 17 at a possible cost of billions of dollars.

The admission is an embarrassment for a society that prides itself on its high-tech skills and has some of


MONEYLIFE NEWS & VIEWS IN YOUR INTEREST

#IL&FS #DHFL #ESSAR #Jet Airways #SEBI #RBI #NCLT #IBC #NSE

Jamaican Supreme Court Strikes Down National Identification Act, Praises Justice DY Chandrachud's Dissent Judgement in Aadhaar case!

Personal Information stolen from National ID Database


ID cards scheme to be scrapped within 100 days

Bill abolishing ID cards and national identity register will be first piece of legislation introduced to parliament by the new government, says Theresa May

Note: Information regarding the ID programs is based on public information available on the respective newspaper websites

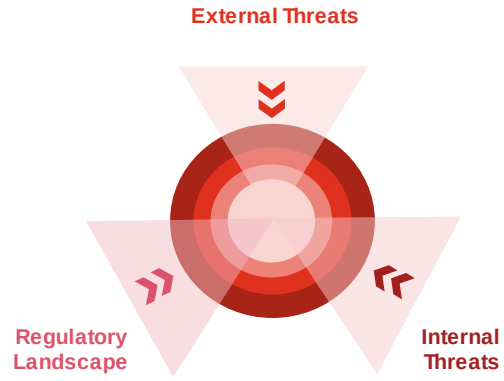
To make it reliable and resilient, managing risk becomes paramount..

Staying Ahead of Risk..

Note: Information regarding the ID programs is based on public information available on the respective newspaper websites

Risk Management -Identify Risks

1 ⚠ | **Risk**

Objective	Identify risks	Assess risks	Determine risk response
How	1 Consider the organizational goals & business drivers of NID 2 Scan the internal & external environment and assets of NID 3 Inventory Threat Landscape 4 Historical & forward-looking analyses 5 Inventory key risks that should be assessed and monitored	**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 Register 

Risk Management - Assess Risks

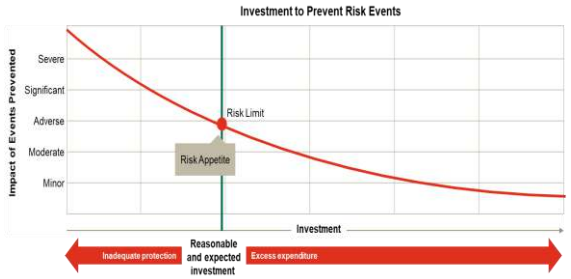
Objective	Identify risks	Assess risks	Determine risk response

How

Risk Classification

Risk Classification	Number of Risks		Critical Risks		% Risk Family Critical	High Priority Risks		Lower Priority Risks		Lowest Priority Risks	
IT Governance	17	13%	6	19%	35%	0	0%	8	15%	3	15%
Information Security	35	26%	6	19%	17%	14	47%	12	23%	3	15%
Biometrics	4	3%	4	13%	100%	0	0%	0	0%	0	0%
Change Mgt	12	9%	3	10%	25%	3	10%	4	8%	2	10%
Quality Mgt	2	2%	2	6%	100%	0	0%	0	0%	0	0%
Architecture	4	3%	2	6%	50%	1	3%	0	0%	1	5%
Compliance Mgt	9	7%	2	6%	22%	0	0%	6	12%	1	5%
Project Management	4	3%	1	3%	25%	2	7%	0	0%	1	5%
Incident & Problem Mgt	5	4%	1	3%	20%	1	3%	2	4%	1	5%
Partner Ecosystem - People	6	5%	1	3%	17%	2	7%	2	4%	1	5%
Authentication Process	7	5%	1	3%	14%	2	7%	4	8%	0	0%
Enrolment Process	8	6%	1	3%	13%	3	10%	4	8%	0	0%
Data Mgt & Document Retention	9	7%	1	3%	11%	0	0%	5	10%	3	15%
Business Continuity & Recovery	6	5%	0	0%	0%	1	3%	1	2%	4	20%
Operations & Support	5	4%	0	0%	0%	1	3%	4	8%	0	0%
Total	**133**	**100%**	**31**	**23%**		**30**	**23%**	**52**	**39%**	**20**	**15%**

Risk Appetite

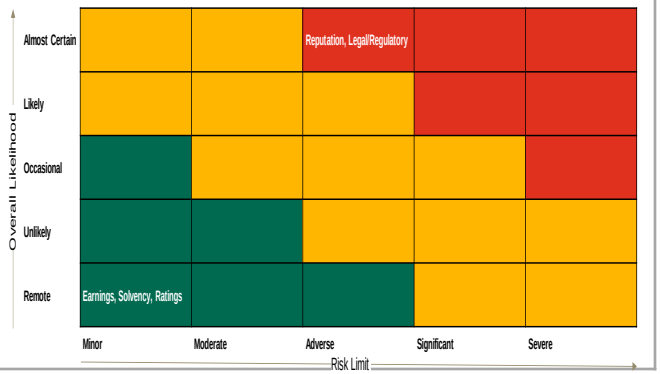


1. Likelihood, impact & correlation using simulations / scenario analyses
2. Identify the interrelationships and concentrations of risk
3. Develop risk rating scales that consider cross-organizational impact
4. Develop a heat map or radar of key risks
5. Update risk appetite and tolerances

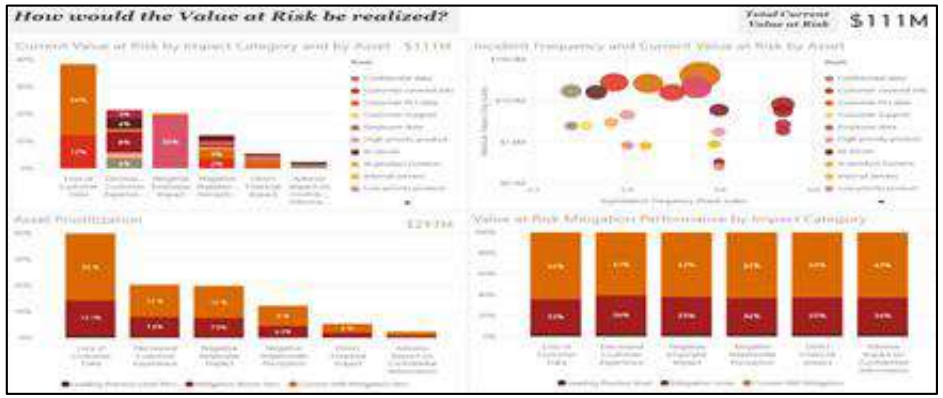
Risk Scenarios

	Sample Risk Scenarios					
Impact Level	Data Breach	Data Corruption	Outage/Disruption	Non-Compliance	Data Loss	Physical Breach
Severe	Full breach of a data center	Complete corruption of a primary data center and its backup(s)	Sustained outage of a primary data center	Non-compliance with multiple regulations across the globe	Complete data loss at a primary data center, including backup(s)	Physical breach of a data center
Significant	Breach of a large office or of sensitive data (e.g., PII)	Corruption of a data center, but not of any backups	Temporary outage of a primary data center	Non-compliance with a regulation applying to an entire region	Loss of personal information at a large office	Physical theft of assets containing unencrypted data (e.g., PII)
Adverse	Breach of a small office (e.g., India)	Corruption of data for a business-critical application	Outage of a client-facing application	Non-compliance with a regulation applying to a small office	Loss of data at a small office	Physical breach of a small office
Moderate	Limited breach of sensitive data (e.g., IP)	Corruption of data for a non-critical application	Outage of a business-critical, internal facing application	Non-compliance with a regulation with no disclosure requirement	Partial loss of data at an office	Physical theft of assets containing unencrypted data (e.g., IP)
Minor	Breach of public or fully encrypted data	Corruption of data on a single workstation	Outage of a non-critical, internal facing application	Non-compliance with unenforceable law or regulation	Loss of data that can be recovered by backup	Physical theft of encrypted assets
Probable Impact	Significant	Adverse	Adverse	Moderate	Minor	Minor
Likelihood	Almost Certain	Almost Certain	Likely	Occasional	Unlikely	Occasional

Heat Map



Risk Management - Determine Risk Response

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

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

2 Governance

Business Requirement | **Laws and Regulations** | **Contractual Requirement**

Accuracy

Privacy

Security

Availability

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

Technology | **People** | **Processes** | **Policy**

..and regular Compliance checks through continuous monitoring and periodic assessment

3 Compliance

Business Requirement | Laws and Regulations | Contractual Requirement

Accuracy | Security | Privacy | Availability

24* 7 Continuous monitoring

- **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

Periodic Assessments

- **Planning**
  - Audit Charter
  - Understand sub process, controls and risk
  - Prepare work program
- **Field Work**
  - Process walk through
  - Conduct testing (walkthrough, observations, enquires etc)
  - Identify gaps
- **Report and closure**
  - Prepare draft report- (observations, risk rating etc)
  - Agree and closure

Forensic

- **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**

Technology | People | Processes | Policy

Technology View to the GRC Solution..

Dashboarding & Reporting

Forensics

- Live Server acquisition
- Integrated Disk forensic
- Password recovery toolkit
- Security investigation
- Forensic Disk duplication

GRC

- Modelling
- Fraud Detection
- **Fraud Management**
- Risk Modelling & Simulation
- IT GRC
- Enterprise GRC

- Incident Management
- Global Intelligence Feed

Security Information and Event Management (SIEM)

Event Correlation & Aggregation

- Database Monitoring
- Malware Analysis (End Point)
- Vulnerability Monitoring
- WebApp Security Assessment
- Network Monitoring
- Malware Analysis (Host)
- Penetration Testing
- SourceCode Security Assessment

Periodic Audits

- BCP/DR Process Assessments
- Security in Change Management
- Physical and Environmental Security Awareness
- SLA Process Assessments
- Root Cause Analysis Assessment
- Fraud Risk Assessment and Fraud Management Process Assessment

Infrastructure

- Network
- Servers
- End points
- Applications
- Databases
- Security Appliances

Partner

AUA	ASA	Op testing & Certification
Enrolment Agencies	Registrars	Device Testing & Certification
Call Center	Others	Logistics

"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