RSAConference2017
Abu Dhabi | 7–8 November | Emirates Palace

POWER OF OPPORTUNITY

SESSION ID: CCS-T07

The Etihad Journey to a Secure Cloud

Georges de Moura
Head of Group Information Security, Risk & Compliance
Etihad Aviation Group

History: Before The Cloud

- Devolved IT Decision-Making
- Traditional Approach to Computing
- On-Premises Apps
- IT Security Controlled The Perimeter
- Believed this was Sufficient to Control Threats & Stop Data Loss

The Clouds are coming

- Challenges:
  - Proliferation of Cloud services (SAAS, PAAS, IAAS)
  - Rise of ShadowIT leading to uncontrollable risks
  - Consumerization of IT (BYOD,…) emergence
  - Finding a balance between productivity, agility and, security
- Risks:
  - Violation of compliance requirements with regulatory laws (GDPR,…)
  - No governance and inadequate due diligence on shadowIT services (supplier, cost, security, architecture)
  - Data breaches which can result in high fines, damage brand and impact revenues
  - Compromised credentials and broken authentication
  - Password fatigue and poor digital hygiene

Visibility, Then Manage

- How Many Cloud Services Are We Using?
- Quick Realization That Use Was Widespread & Uncontrolled
- Identified Risks (Technical, Legal, Data, User etc.)
- Needed To Assess Risk of Each Service
- Outcome: We Have To Manage Cloud, not Avoid or Eliminate, but Control

Managing the Cloud

- Establish a clear Cloud strategy policy that defines the adequate controls to be in place depending on the data sensitivity and regulatory requirements (GDPR, NESA,…)
- Extend your security services to Cloud environments to provide visibility and manage
- Implement a risk management framework that cover Cloud providers
- Block non sanctioned high risk cloud services
- Select certified Tier-1 cloud providers to host your most sensitive data

Cloud Security Governance

- EAP Cloud Security Strategy and Policy
- Governance, Risk and Compliance Management processes for Cloud services (CSA, ISO27018)
- IDAAS for SSO and Secure authentication of Cloud services
- CASB for ShadowIT visibility
- CASB for monitoring and data protection

Cloud Security Strategic Objectives

The Public Cloud Security solution must be an integrated extension of Etihad's Security ecosystem that includes **Security incident management, Security monitoring, data leakage prevention, and data encryption.**

The Public Cloud Security solution must work as a **policy enforcement point** between the cloud applications and the consumers in order to achieve **consistency of the Security controls, visibility** and **compliance.**

The Public Cloud Security solution must provide **visibility and control** to reduce the risk of adopting Public Cloud services.

The Public Cloud Security solution must provide **secure access** from any device or from any location.

Benefits of IDAAS and CASB solutions

Consolidation and standardization
Visibility into the usage of unsanctioned cloud applications can help identity redundant services

Understand the Business needs
Better align with business requirements by having insights into cloud applications usage

Enable the Digital Transformation
Improve the connections between people and tools to make the Organization more Productive and Secure

Drive Business value
Protect content that has business benefits in order to drive business value and improve cloud adoption: Just-in-Time provisionning, SSO, remove password management headaches

Security powered by the Cloud
Faster delivery, scalable, simplified architecture, predictable TCO, leverage cloud security experts

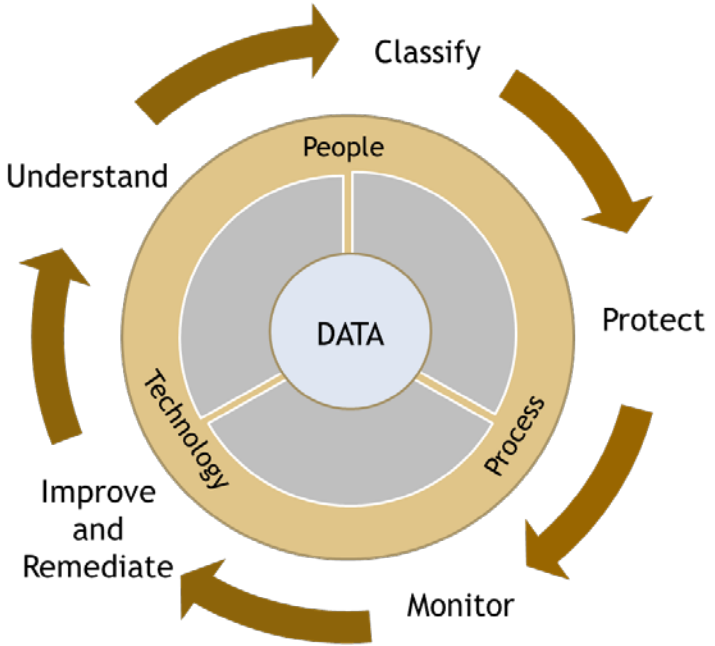
Extension of current controls environment
Identity management, access management, monitoring, DLP, encryption

Improved Compliance
Identify áreas that may expsose the Organization to regulations (GDPR) and fine and enforce required security controls

Mitigate risks of Security breaches
Protect the Organization against Internal and External threats

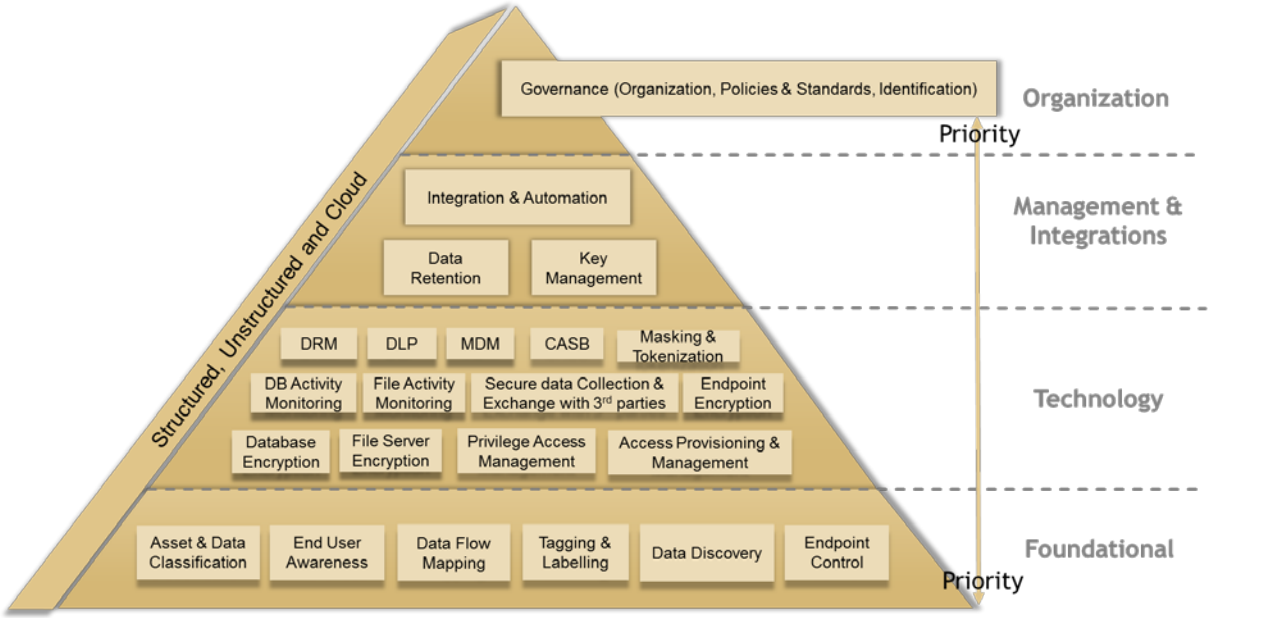
Build a holistic Data Security Program

Maximize Technology Investment
Building a data protection program that is aligned to the business
Implementing an effective program structure
Spending time, energy and money protecting the data that matters most
Changing the business culture and measuring performance to achieve sustainability



Data protection is a holistic program involving all the organizations users and not a technology project

Build a solid foundation



Think big, start small and grow gradually for full coverage

Spent your time and money protecting the data that matters the most

- Detect and prevent inappropriate transfers of sensitive data from the internal network to the internet
- Ensure that authorized transfers of sensitive data are appropriately encrypted
- Identify and secure data at rest
- Control endpoints, including workstations and mobile devices

Technology is not a magic bullet

Change the culture and measure performance

- Build a culture of data protection
- Establish meaningful metrics
- Report to the business and continually improve
- Allow Collaboration Internally & External, but with Controls
- Senior Management Support Crucial
- Strong Message to Users Around Central Management & Control

Cloud Security is a Team Sport

Cloud Security: Advice For Your Journey

- Establish a Cloud Security Framework
- Ensure effective governance, risk and compliance processes exist
- Manage people, roles and identities
- Ensure proper protection of data and information
- Enforce privacy policies
- Assess the security provisions for cloud applications
- Ensure cloud networks and connections are secure
- Evaluate security controls
- Senior Management Support is Crucial

الإتحاد
ETIHAD
AVIATION GROUP

THANK YOU