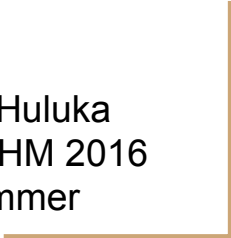




# Cloud Control Matrix for Secure Cloud

By: Daniel Huluka  
NeIC AHM 2016  
Lillehammer



# Assets in the Cloud

Assets in the cloud (the view from cloud customer and cloud provider)

1. Data
2. Applications/Functions/Processes
3. Infrastructure
4. ...

# What makes Cloud Security Different?

- Accountability
- Giving / Taking over control
- Service delivery model (shared resources)
- Cost effectiveness vs security requirements

# Top Cloud Specific Security Risks, ENISA, 2009

1. Loss of Governance
2. Lock-In
3. Isolation Failure
4. Compliance Risks
5. Management Interface Compromise
6. Data Protection
7. Insecure or Incomplete Data Deletion
8. Malicious Insider

# Cloud Top 10 Risks, OWASP, 2010

1. Accountability and Data Ownership
2. User Identity Federation
3. Regulatory Compliance
4. Business Continuity and Resiliency
5. User Privacy and Secondary Usage of Data
6. Service and Data Integration
7. Multi-Tenancy and Physical Security
8. Incidence Analysis and Forensic Support
9. Infrastructure Security
10. Non-production Environment Exposure

# The Notorious Nine CC Threats, CCA, 2013

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

# Impact?

Cloud confidence is rising!

“64.9% of IT leaders think the cloud is as secure (47.1%), or more secure (17.8 %) than on premises software.”

Source: THE CLOUD BALANCING ACT FOR IT: BETWEEN PROMISE AND PERIL

Survey by CSA and SKYHIGH NETWORKS

# Standards and Frameworks to Mitigate Risks

- HIPAA and HITECH Act
- ISO/IEC 27001, 27017
- NIST SP800-53 R3
- PCI DSS 2.0
- GAPP (Generally Accepted Privacy Principles)
- Jericho Forum
- FedRAMP (Federal Risk and Authorization Management Program)
- ...



# Cloud Control Matrix

- Fundamental security principles
  - to guide cloud vendors towards secure cloud service
  - to assist prospective cloud customers in assessing the overall security risk of a cloud provider
- Maps to the requirements of most of the available standards
- It has two major versions
  - V 1.0 (98 controls in 10 domains, published in 2010)
  - V 3.0 (133 controls in 16 domains, published in 2014)
- As the stakeholders in Glenna are both cloud consumers and cloud service providers on different scenarios, we found it to be a good building block in security related tasks in the project.

# Cloud Control Matrix ...

## CCM v3.0.1 DOMAINS

<b>AIS</b>	Application & Interface Security	<b>HRS</b>	Human Resources Security
<b>AAC</b>	Audit Assurance & Compliance	<b>IAM</b>	Identity & Access Management
<b>BCR</b>	Business Continuity Mgmt & Op Resilience	<b>IVS</b>	Infrastructure & Virtualization
<b>CCC</b>	Change Control & Configuration Management	<b>IPY</b>	Interoperability & Portability
<b>DSI</b>	Data Security & Information Lifecycle Mgmt	<b>MOS</b>	Mobile Security
<b>DSC</b>	Datacenter Security	<b>SEF</b>	Sec. Incident Mgmt, E-Disc & Cloud Forensics
<b>EKM</b>	Encryption & Key Management	<b>STA</b>	Supply Chain Mgmt, Transparency & Accountability
<b>GRM</b>	Governance & Risk Management	<b>TVM</b>	Threat & Vulnerability Management

**136 CONTROLS**

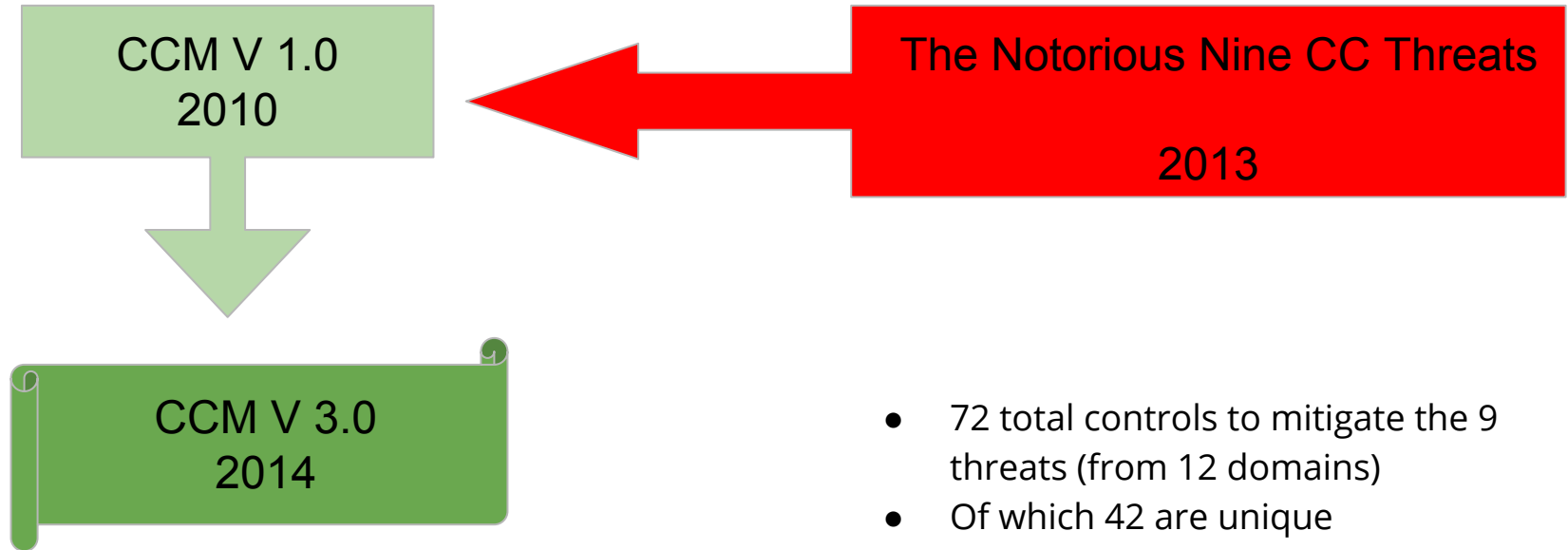
Cloud Controls Matrix v3.0



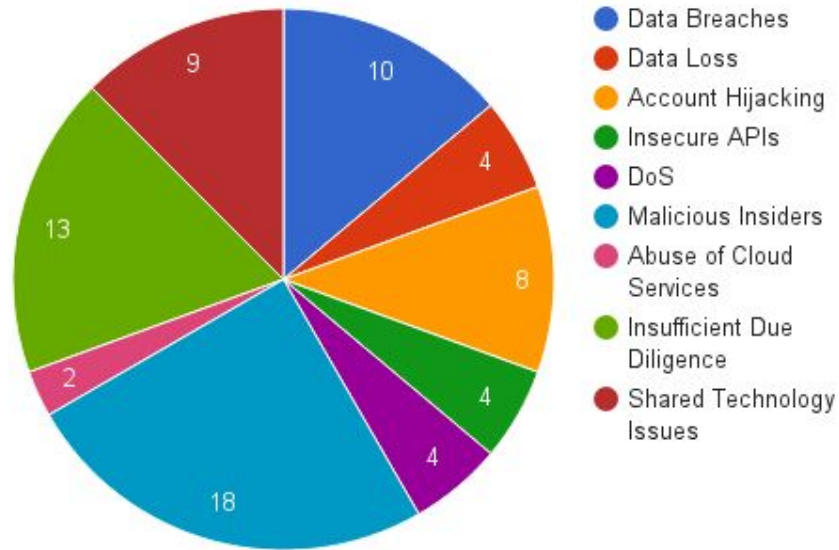
**133 CONTROLS**

Cloud Controls Matrix v3.0.1

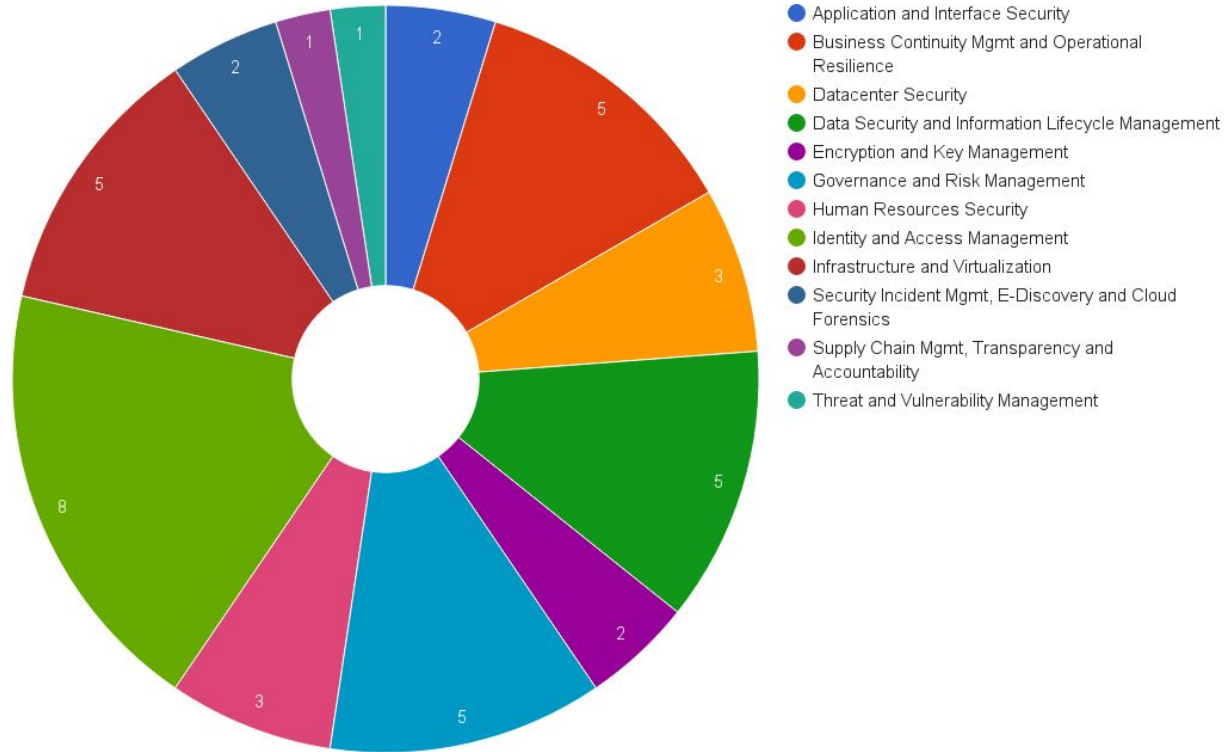
# Mapping Cloud Controls



# Number of Required Controls to mitigate each Threat



# Number and Domain of the selected controls



?