Towards a Common Goal

Ensuring Security in Cloud Environments

CDSA CONTENT PROTECTION SUMMIT
December 4, 2019
Sheraton Universal | LA

convergent

Leaders in Risk Assessment & Mitigation

Providing Security Consultancy for Cloud Hosted Environments

Cloud Compliance
Chris Johnson, CEO
Methodology
Janice Pearson, VP Global Content Protection,
Engagement
Mathew Gilliat-Smith, Advisor

Cloud Compliance

By Chris Johnson, CEO

convergent

convergent

Fact or Fiction?

‘Some Say’ the cloud is the ‘the place to be’; user friendly, fast, efficient and economically friendly

‘Some Believe’ that behind the fluffy white façade lurks a dark and sinister threat; on prem remains the safest most secure place for content to reside only trusting certain cloud-based activities due to their increased efficiency and to remain competitive

‘We know’ that done correctly with the right; planning, preparation, monitoring and maintenance both eco systems can securely co-exist in harmony and; dependent upon the need a cloud environment can boost productivity, supercharge delivery, reduce overhead and even improve security!

But how can this be achieved?

convergent

Cloud Security

If correctly configured and where relevant best practice is followed, cloud workflows create undisputed speed, cost and security benefits

If not done correctly, serious security pitfalls occur (e.g. unrestricted access; weak encryption, exposed keys)

Why is it so difficult to get security right in the cloud?

ISO, NIST, ISACA, COBIT, CSA. SANS, DPP, TPN, MPAA, (BP) NCSC, AWS, AZURE, GOOGLE, IBM

Each user case is different, many types of user configurations & varied control frameworks. It's complex and confusing.

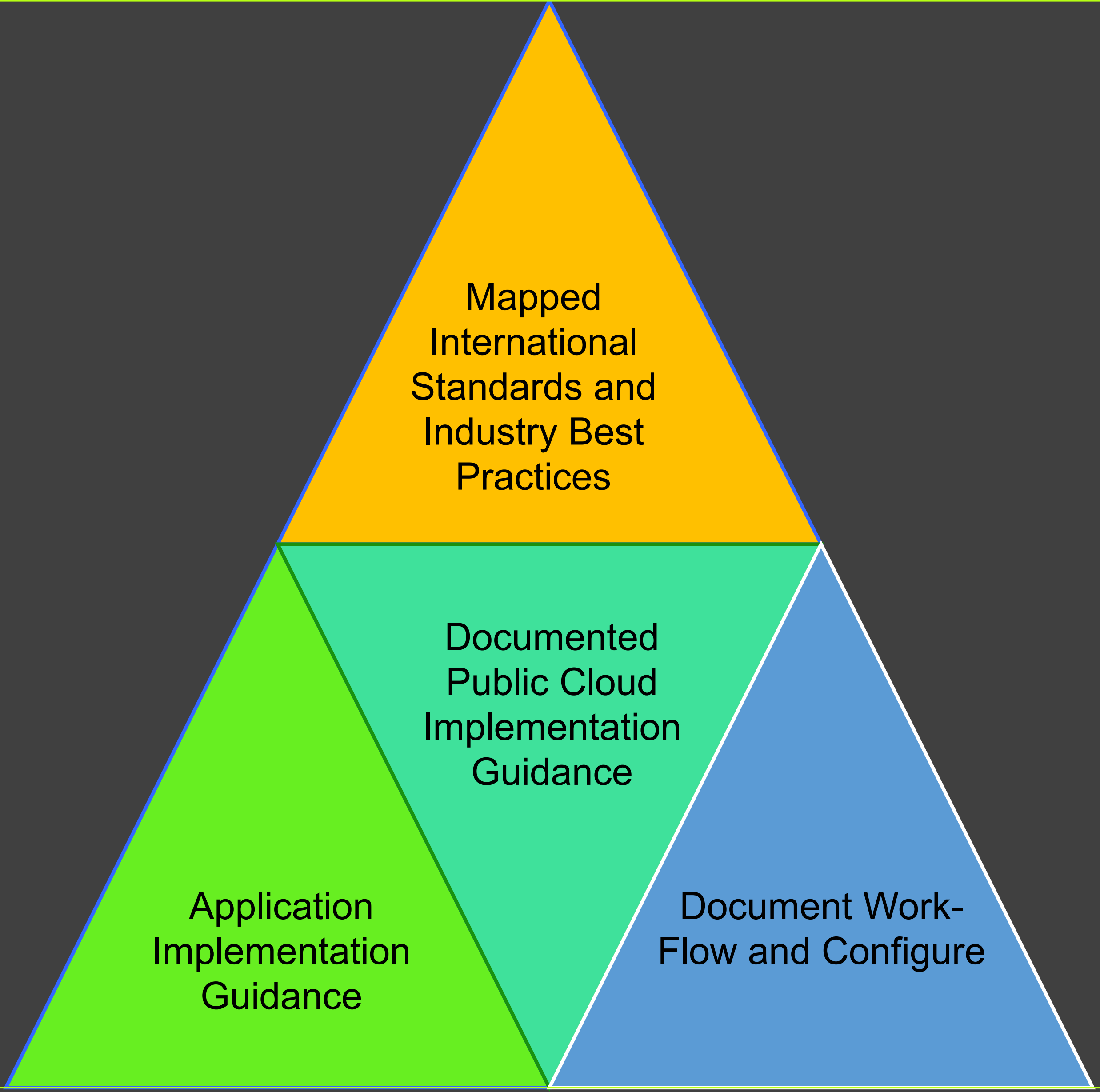
This is where the issues exist

convergent

“I just need some cloud security 101 practical advice?”

- Know your business requirements
- Understand your information
- Determine relevant security principles
- Understand how the principles are implemented
- Understand the level of assurance offered
- Identify additional mitigations you can apply
- Consider residual risks
- Continue to monitor and manage the risks

Existing Guides Already Available



Mapped International Standards and Industry Best Practices
Documented Public Cloud Implementation Guidance
Application Implementation Guidance
Document Work-Flow and Configure

Methodology

By Janice Pearson, VP Global Content Protection

convergent

convergent

Methodology Overview

- Discovery
- Architecture Review
- Review Workflows
- Final Scope Review
- Penetration Testing
- Conduct Full Assessment (CSA & supporting frameworks)

convergent

Discovery

What Problems Are We Trying To Solve?

Security Cartography

- Conduct security and compliance mapping aligned to a control framework (e.g. CSA CCM, NIST, OWASP, ISO)

Tasks

- Develop control objective
- Develop an initial security baseline
- Create a responsibility assignment matrix specific to cloud ("RACI"), which maps the people who are **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed within the organization

Output (via Consultancy)

- Document controls based on the chosen framework
- Development security baseline documentation
- Remediate high risk items

convergent

Design

Approaches To The Problem

Threat Model exercises

- Across all user stories

Integrate Automation

- Reduce the human element

Documented System Development Lifecycle (“SDLC”)

- For consistency throughout the system’s lifecycle (applications)

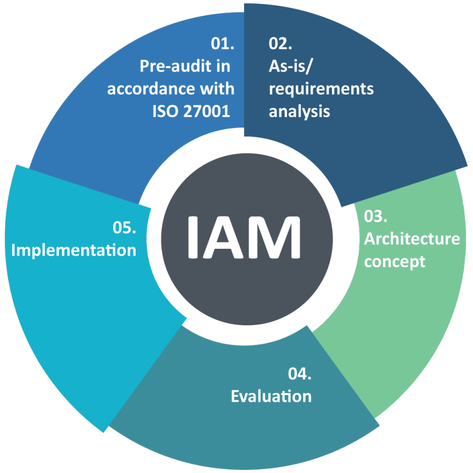
Output

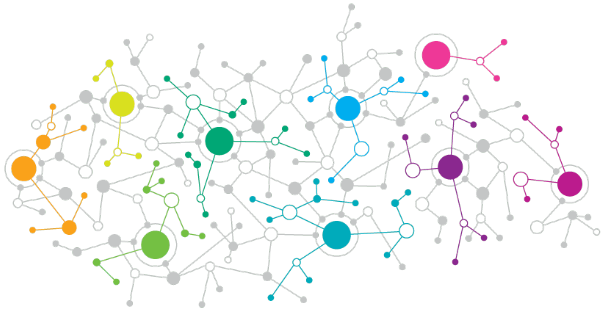
- Identify Control Actions
- Playbook Generation
  - IAM, Detective Controls, Infrastructure Security, Data Protection and Incident Response

convergent

Tackling Security for Individual Areas

- Logging & Monitoring
- Access Management
- Networking
- Managed Services


IAM
01. Pre-audit in accordance with ISO 27001
02. As-is/ requirements analysis
03. Architecture concept
04. Evaluation
05. Implementation



convergent

Implementation

+

Actionable Tasks

- Regular training & testing
- Aggregation of security information
- Monitoring of all sources of AWS Security telemetry
- Iteratively develop control capabilities

Engagement

By Mathew Gilliat-Smith

convergent

Everyone is Different

1. All in the Cloud
   - Replicate on prem in the cloud hosted environment (multiple copy)
   - Centralised storage is preferred
   - Forgo security for performance

2. Hybrid – Cloud/On Prem
   - Constant hand-off of content through workflow increases risk

3. Thinking About It /Transitioning
   - Mixed approach &/or legacy open risk
   - Still deciding on which options

Engagement

Listening to operational stakeholders

Agreeing the scope

Testing

60% Overall Compliance

Mapping relevant best practice & reporting

Recommendation for enhancements

Implementation

convergent

Ongoing

Providing specialist technical security consultancy and compliance for cloud workflows

Support

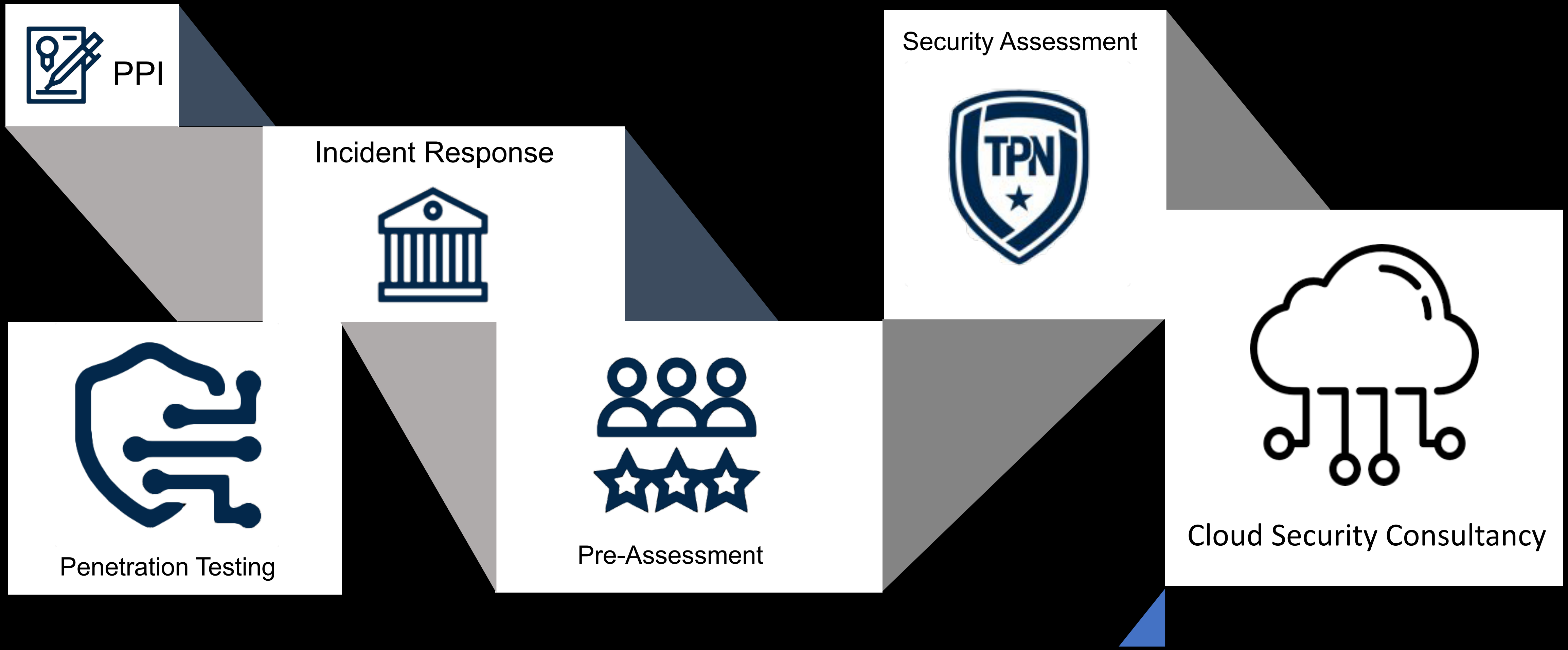
- Delivering Strategic Support and operational solutions for the secure, safe and uninterrupted delivery of media assets in cloud workflows for major studios and their supply chains

Assurance

- Ensuring that you are secure in each of your workflows and where you interconnect with third parties

New or Altered Standards

- Utilising Knowledge and Experience of new & changing International Security Standards and media industry best practices for workflow implementation and process integration


PPI

Incident Response

Penetration Testing

Pre-Assessment

Security Assessment

Cloud Security Consultancy

About Us - Risk Assessment & Mitigation

convergent