Cisco Cloud Assessments

Justin Tang

Agenda

Cisco Landscape

Evolution of Cloud Assessments

Performing Cloud Assessments

Challenges

Cloud Service Providers at Cisco

Definition:

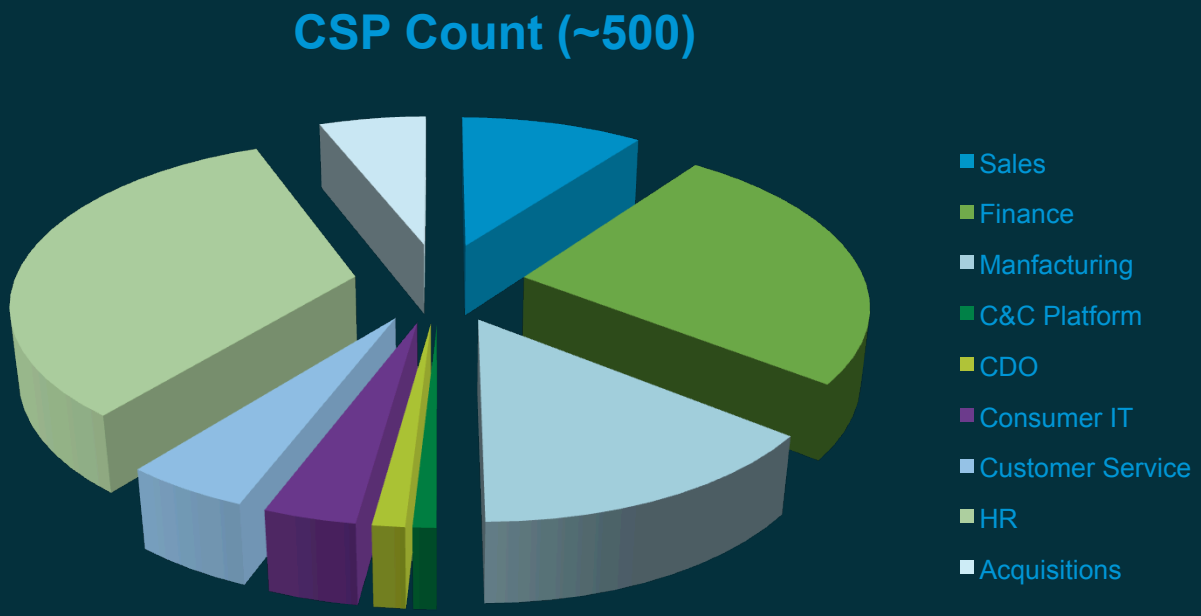
The service handles or hosts data that Cisco owns or has a fiduciary responsibility to protect and/or

The external site(s) might be considered by a user to be a part of Cisco's Web presence (internal or external)

Types of Cloud Service Providers include, but are not limited to, the following:

Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) & Cloud Infrastructure as a Service (IaaS)

Cisco's External Cloud Provider Usage

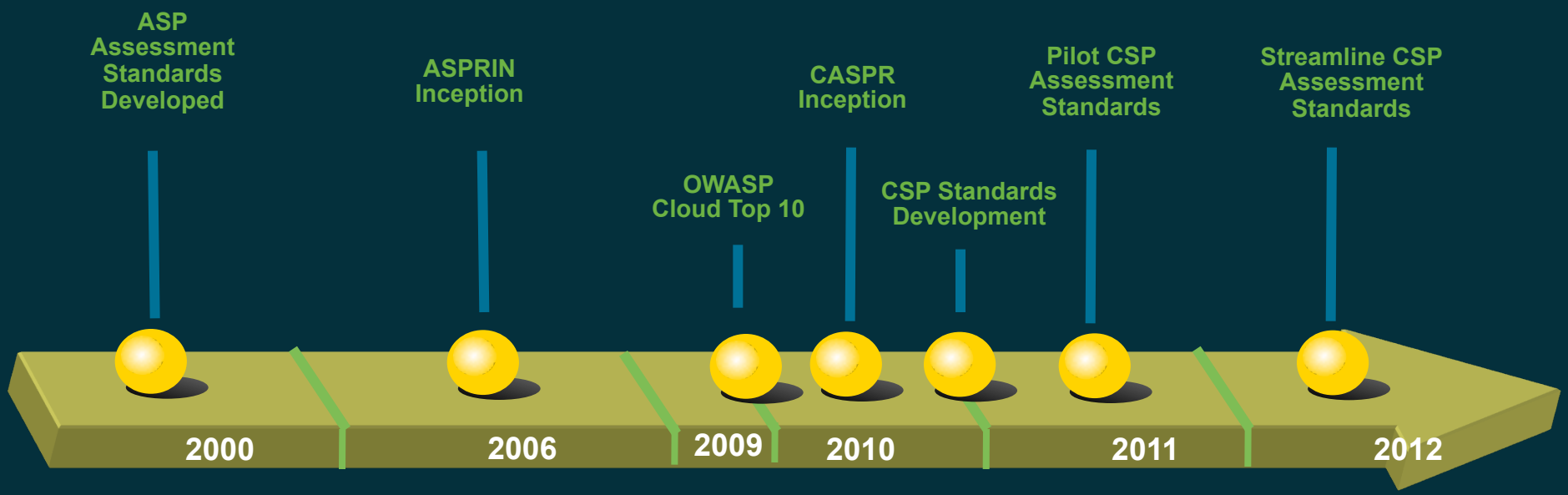


Business Drivers for CSPs
- Cost

- Time to Market (Speed)

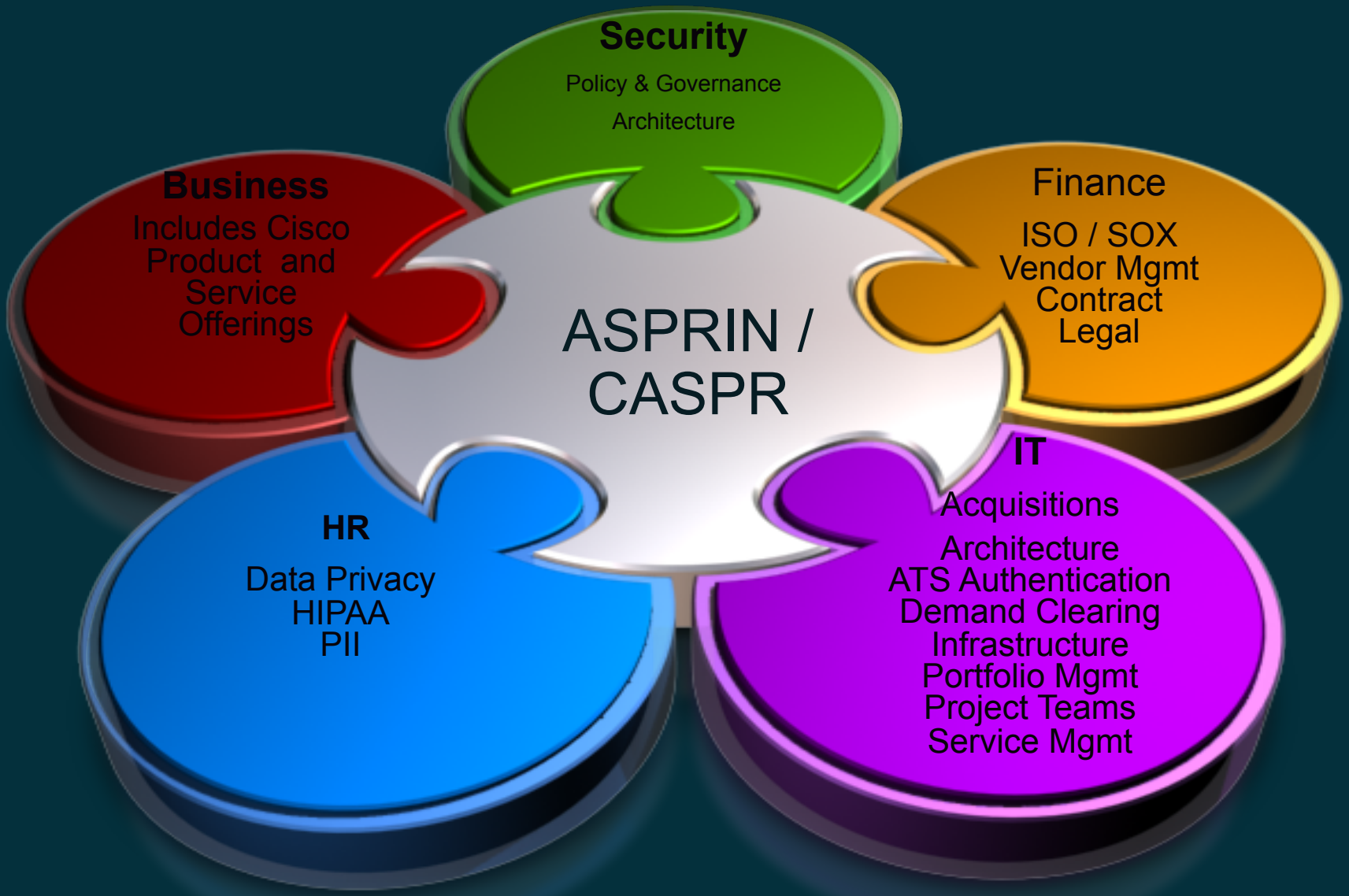
- Specialized Service

Cisco's Evolution of Cloud Provider Assessments



ASP – Application Service Provider
ASPRIN – ASP Remediation Initiative
CASPR -- Cloud Service Provider Reviews

ASPRIN/CASPR – Enterprise Wide Program



Performing Cloud Assessments

CASPR Review Lifecycle

CASPR PM holds CSP Discovery Meeting

InfoSec Informs GCM of Security Approval

GCM informs IT of CSP Agreement Signing

TBD based on scope

Engage SMEs → **Security Review** → **Contract Work** → **Integrate Vendor**

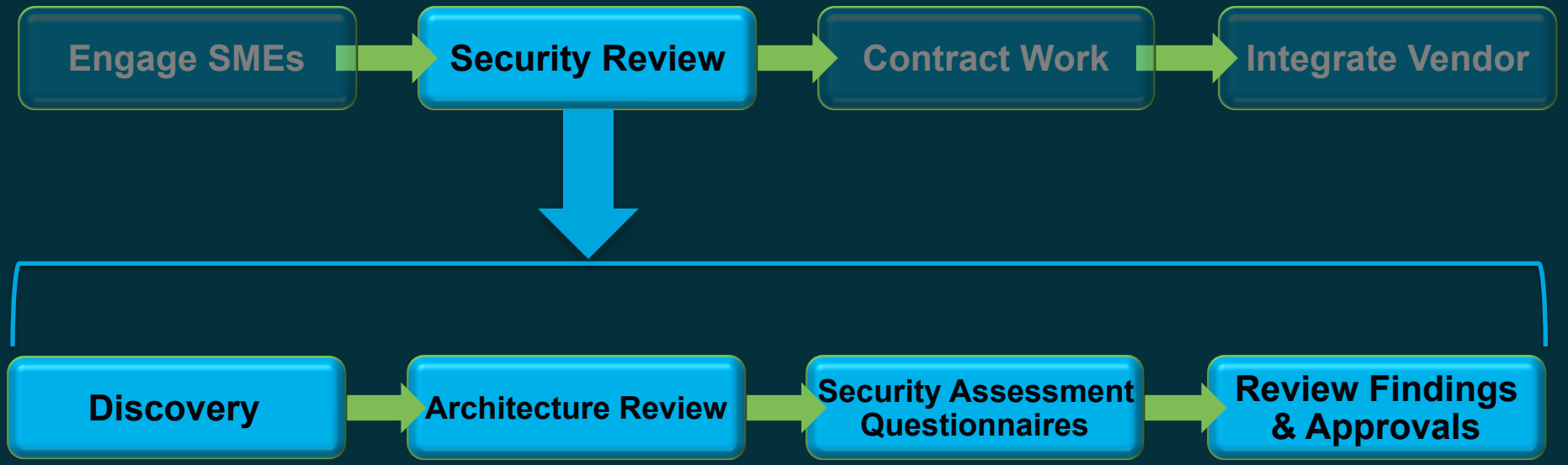
- SMEs within functional groups
- Obtain Business & IT VP Approval
- Complete Requested Forms & Diagrams

- Security Assessment

- Business lead and Global Contracts Management (GCM) negotiate contract with vendor

- Implementation of vendor solution
- Renewals

CASPR Security Review Lifecycle



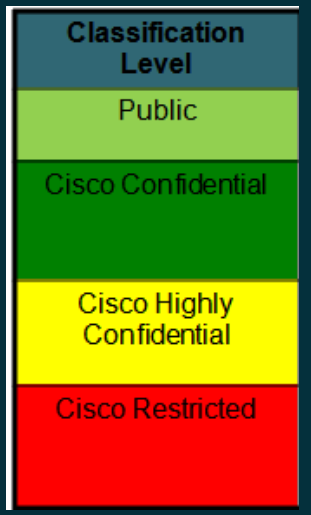
CASPR: Discovery

Example: Collecting Cloud Tier Ownership

Service Tier Ownerships				
Cloud Layer	Who owns this tier?	Multi-tenancy at this layer (Yes/No)	Who owns the management/ operations of this tier?	Who has Security Responsibility?
SaaS				
PaaS				
IaaS				
IaaS (2)				

Example: Collecting Data Details

Cisco/Customer Data	
Data Classification and Sensitivity	Provide details on the Cisco data that will be hosted on the Cloud vendor using Data Sensitivity template.
Data - Physical Location	What will be the physical/geographical location of data in cloud?
Data Flows	Data Flow Sample
Regulatory Data	Provide details on what regulatory and privacy (PII) data will be handled
Customer Data	Provide details on what customer data will be handled , you can use the data classification template above to specify it.



CASPR: Architectural Review

Data Flows

- Data Flow Paths
- Data between systems/entities

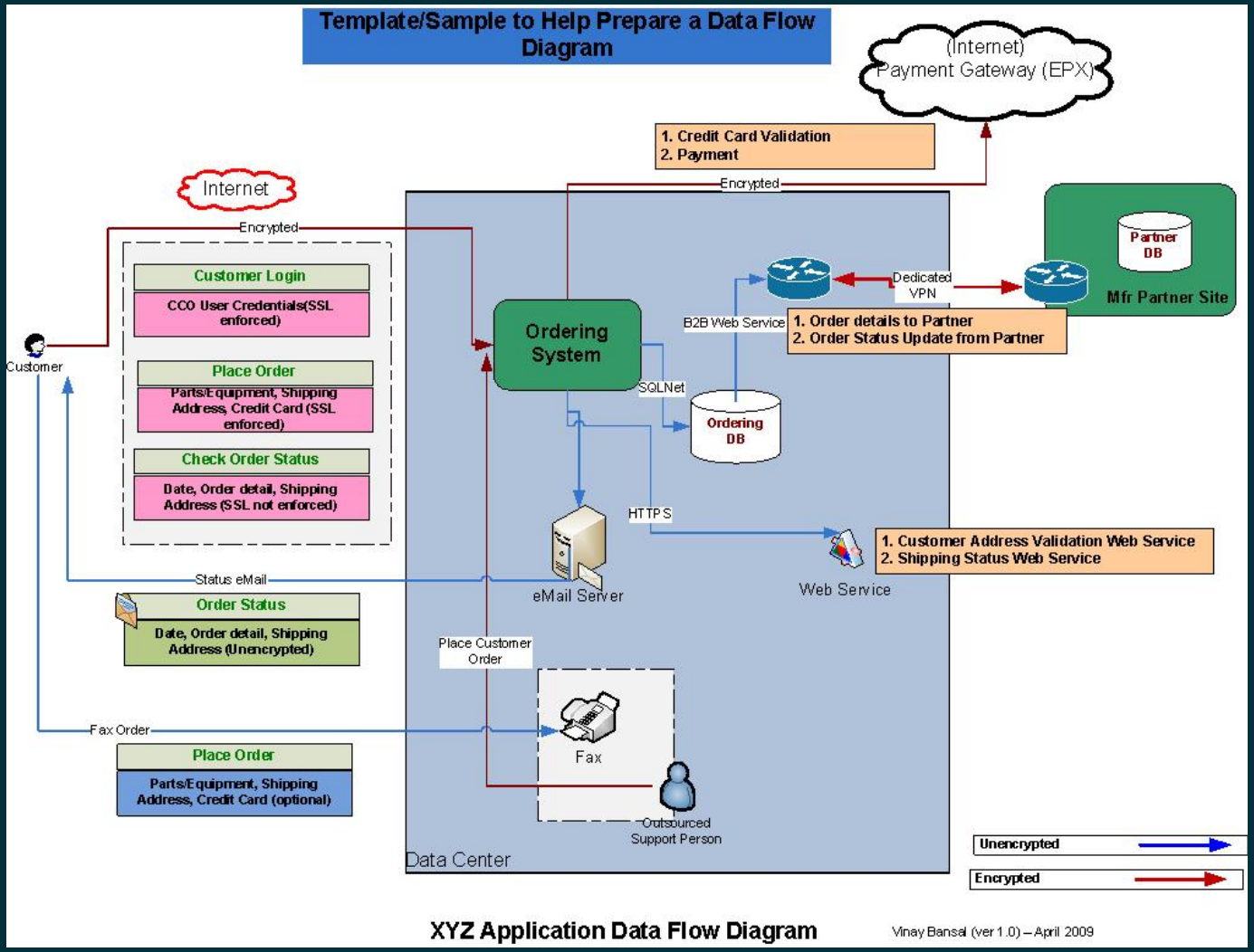
System Architecture

- Logical and Physical
- Security Responsibility and Accountability

Integration Architecture

- Integrations with other systems
- Reach-back Model

Data Flow Template



CASPR: Security Assessment Questionnaire

CASPR: Security Assessment Cisco Standards

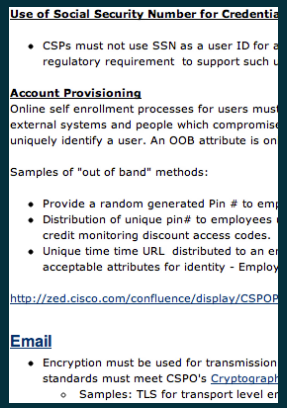
- Overlay the industry standards with Cisco standards.
- Legacy processes and solutions internally and in the industry
- Published internal wiki of standards to address unsecure practices that were being repeated.
- Push these standards into RFPs and vendor selection upstream.

"We work with many fortune 500. Cisco is the first to require this."

"Other customers are okay with it."

"We've never had an incident based on this model."

"We agree, but that's just not how we've done it."



Use of Social Security Number for Credentia

- CSPs must not use SSN as a user ID for a regulatory requirement to support such u

Account Provisioning

Online self enrollment processes for users must external systems and people which compromise uniquely identify a user. An OOB attribute is on

Samples of "out of band" methods:

- Provide a random generated Pin # to emp
- Distribution of unique pin# to employees credit monitoring discount access codes.
- Unique time time URL distributed to an e acceptable attributes for identity - Employ

http://zed.cisco.com/confluence/display/CSPOP

Email

- Encryption must be used for transmission standards must meet CSPO's Cryptograph
  - Samples: TLS for transport level e

CASPR: Review Findings and Approval

Findings

- Security Requirements and Recommendations
- Alternate Controls
- Risk Exceptions

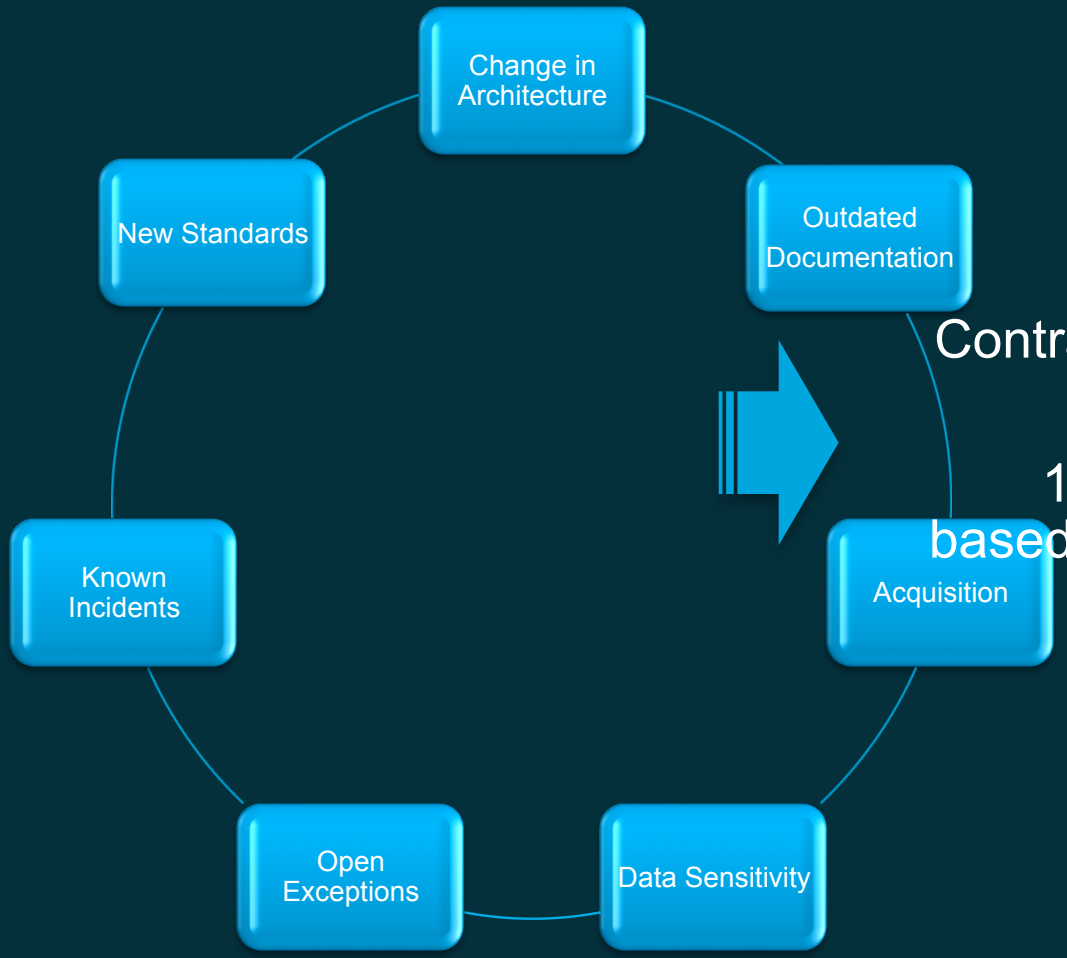
Approved Integration Models

- Federated Auth
- Data Integration
- Administrative Access

Periodic Assessments

- Monitoring/Audit Log
- Vulnerability Assessments
- Incident Response

Triage: Revalidation of CSPs



Contract Renewal Date

1 or 2 years
based on risk ranking

Challenges

Challenges

- Availability of Non-production
  - Integration and functional testing and vulnerability assessment
- Authorized Vulnerability Assessment
- Incident Analysis and Forensic Support
  - Better visibility into CSP environments for proactive monitoring and quicker response.
- Web Application Firewall
  - Evaluation of CSPs ability to support a Web Application Firewall

Availability of Non-Production Cisco Incident

- Site Mistaken for non-production, which did not exist.
- CSP hosted site accidently hacked by planned vulnerability assessment
- A scheduled audit and penetration test on improperly inserted factious data into production databases instead of the development version.

Incident Analysis & Forensic Support Mitigation

- ✓ Cloud providers synched up with the enterprise incident response procedures
- ✓ Roles and responsibilities defined
- ✓ SLAs on access to logs
- ✓ Environment isolation for forensic analysis

Thank you.