SECURITY&TRUST
Cloud Security

Unified Compliance Program

Facilitated Compliance Management FCM

Robin Basham, Unified Compliance Program Manager, Lead Archer Architect

Facilitated Compliance Management is an EnterpriseGRC Solutions Approach

Agenda list

1. Unified Compliance Vision
2. What's Wrong
3. How We Fix It
4. Integration Progress – Facilitated Compliance Management
5. Common Assurance Framework Program and Progress

Being secure is enough – Our posture is our brand

Vision – Sustainable Compliance as a Service

Strategy

- Compliance enables and extends market by removing sector, removes regulatory compliance blockers
- Cloud Security Certifications within Government, Finance, Medical, and International Sectors informs how we sell to and support our customers

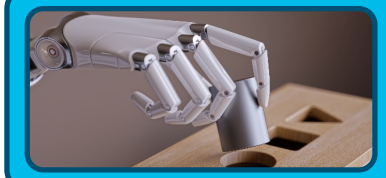
Execution

- Tie out stakeholders, products, policies, goals, control assertions
- Tie controls to common evidence and evidence to common controls
- Build consumable compliance data warehouse
- Visualize every element that adds up to assertions of Compliance

Metrics

- Percentage and Number of Evidence / Test Re-use
- Mapped Policy – policy re-use
- Reduced time to prove and maintain secure operations
- Increased number of externally validated compliance assertions

Common Control Assurance Methodology



Process & Policy Assignment

- Primary Process Owner and Policy Owner
- Sub process inputs and outputs, assets, owners

Mapping to Control Universe

- Match intent of overall objectives – map their outputs
- Align test steps across this and other implemented test methodologies

Associated Question Bank

- Confirm coverage
- Document increased scrutiny

Current Assessment Portfolio

- Company represents “Secure” Products and Services
- Desires Certifications that validate and expand our regulated markets
- To meet these objectives InfoSec & Assurance involve the BU in 6000+ touch points that collectively represent their annual compliance (evidenced by sampled process and technology)
- Interfacing externally to make 1800 control assertions per BU

We ask “Do we have what we need for the audit?”

Tell me if we have everything we need to meet with an external auditor on this <date>, for this <audit>, for this <product>, and for a set of <processes> and their assessment specific <controls>.

Answer by showing the set of <tests> and their <artifacts> as evidence to support our statement that a control, for a particular product, and for a period of time, is READY to pass audit.

You Must Be “This Tall To Ride this Ride”

People Process Technology

- Stakeholders, Auditors, SME, Owners
- Owners produce policy
- Policy drives the organization and its commitments

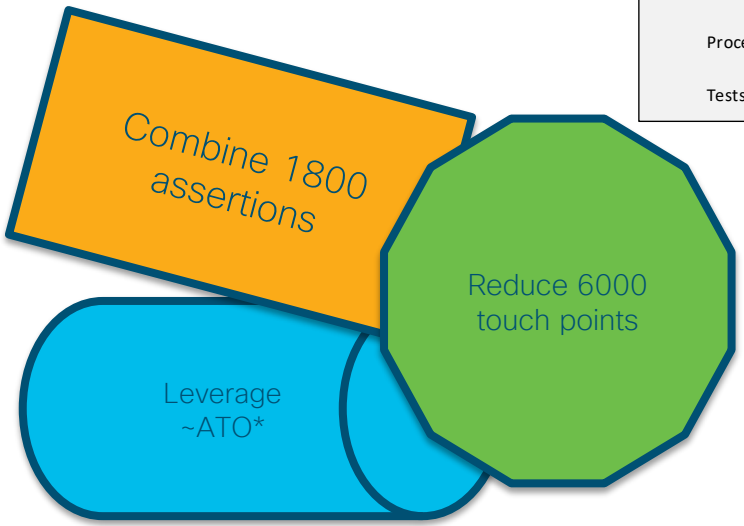
Evidence

- Artifacts in a controlled resource represent single source of truth that a control is happening – but which one(s)?

Assessment

- Framework controls make assertions that processes are happening, details necessary to demonstrate control effectiveness. Tests gather proof of ongoing audit.

Current Product Assessment Portfolio – in DB – still too many things



Control (900)

- PK Assertion
- Policy
- Procedure
- Tests (1 to 50+, average 5)

Test (1982)

- PK criteria from policy
- supporting policy 1or more
- technology - systems 1 or more
- work instruction - 1
- array of properties varies, av. 5
- evidence of use 1, 2, 4, 12 sets of unlimited artifacts

Policy (200~)

- PK Scope
- Control Mapping
- Authority and Duration

Technology (75~)

- PK baseline
- operational procedures
- ACL
- owners, operators

Evidence (Jira plus Doc Central

- PK EDCS (link)
- Type (ties to location)
- Rate (ConMon) frequency expected per period of time

Things under management, 125 Evidence folders, Expectation 4 sets of evidence times each product. Cato is 121 sets of artifacts in each ticket
Estimate 250 x 4 = 1000 things per product

User Experience

How do we make it feel like less?

How do we make all these moving parts consumable?

Product Compliance Portfolio

Removing the ADD in AUDDIT

Dedicated internal Controls Assurance Framework CAF;
Dedicated Cloud product specific Authority to Operate

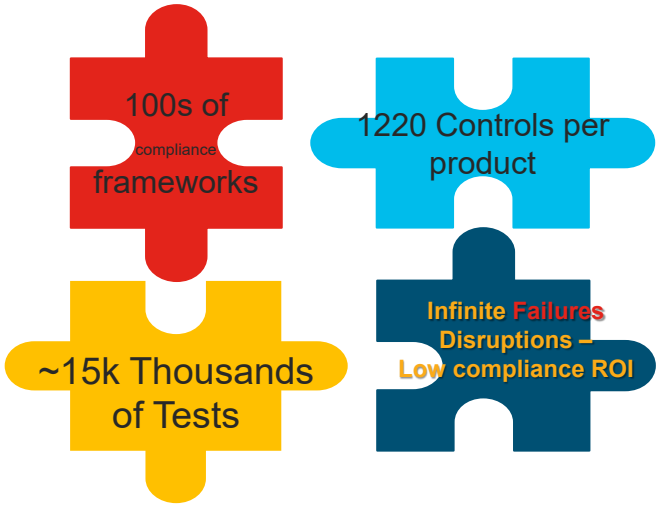
“Am I crazy, or have I answered this question before?”

The “ADD” in AuDDit and the Business Disconnect

- Markets ask *questions* using different language, context, boundary, and depth
- The Security *answers* constantly change, products change, and market demands change
- Reactive compliance fractures business strategy

Making Connections

- Replace the barrage of compliance questions with one connected process
- Control Assurance framework integrates requirements, catalogs capabilities, organizes evidence
- Control Assurance Framework ensures each business experiences a unified, integrated one stop compliance shop



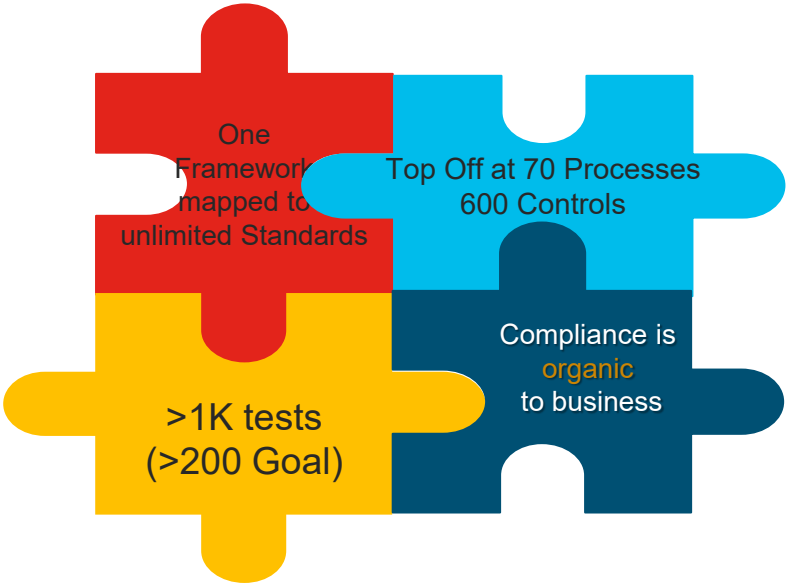
No, …you're not crazy.

Controls Assurance Framework = Dedicated Support

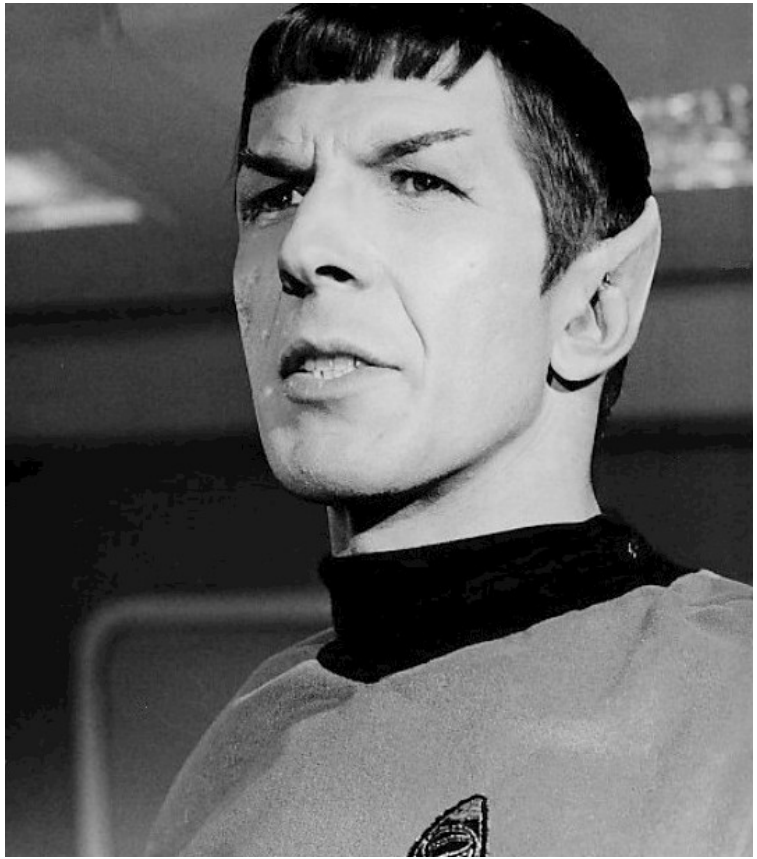
Every market uses different questions to get at the exact same answers (outcomes). To get ahead of insanity, we manage the answers.

Leveraging Connections

Instead of subjecting our product BU to constantly shifting compliance requirements, a custom internal Control Assurance framework gathers all of it, produces a single assessment methodology, maps all the evidence (outcomes), and engages in meaningful risk discussion around better process.



SPOC not Spock



Common Control Assurance Framework keeps you sane

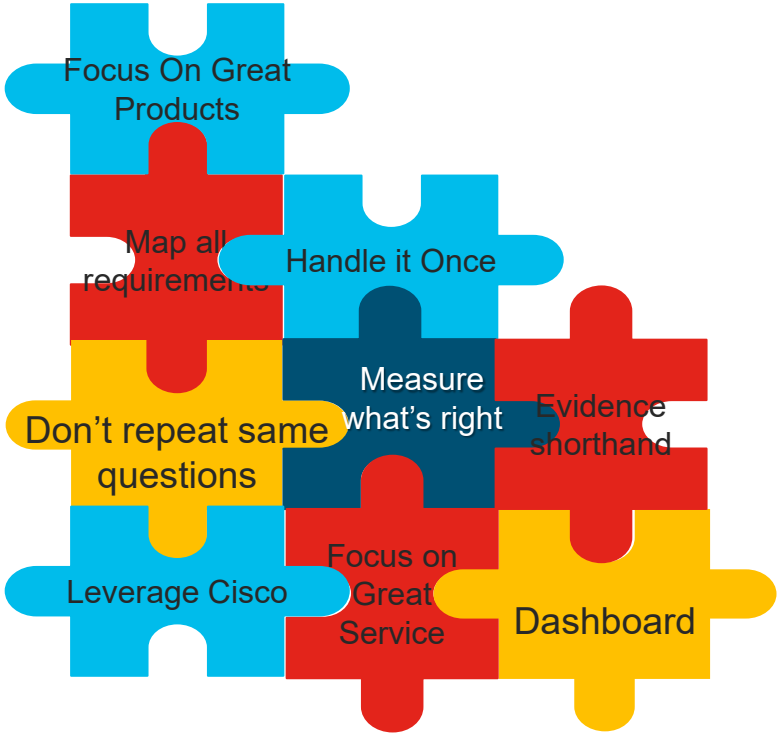
Sanity through connection and retention

- One team acts as your product's SPOC helping to navigate your evolving compliance portfolio
- Assessment captures in one set of procedures all major processes – satisfies ALL externally audited frameworks

Less Disruption = Better Practice

- Business need straight forward guidance – current policy, process and standards for their job.
- Your BU are the experts. They deserve continuous credit for all their hard work – capture their outcomes

**Why "Better" not "Best"? Because "better" is about right bar for the right business goals, and best is just enough to maintain a healthy risk appetite.*



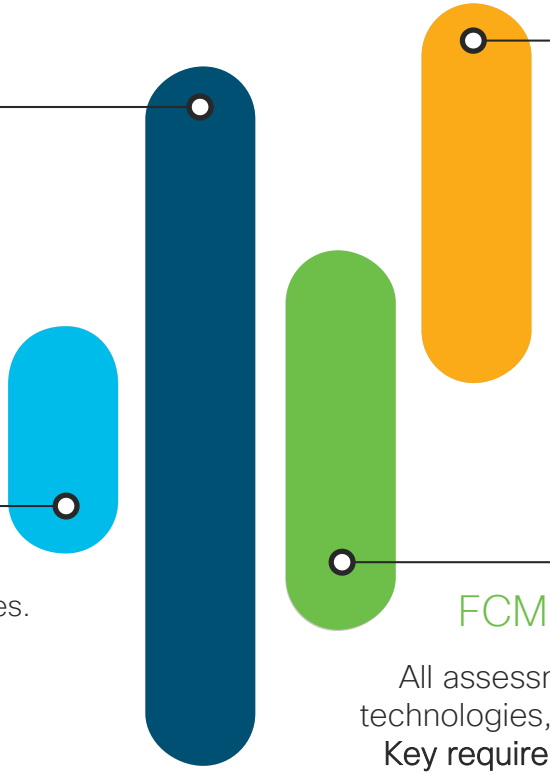
Facilitated Compliance (FCM) Main Components

Unified Process Based Risk Assessments

All security assessments align with our major attestations and certifications. We map to either NIST, ISO27001/2002, SOC2, and ~ATO*. Special assessments consume common controls from these major compliance events.

Policy Life Cycle Management

Policies, Procedures, Standards, Guidelines. Policy lifecycle includes mapping policy assertions to major frameworks, adding a service that supports policy continuous optimization.



Risk Analysis

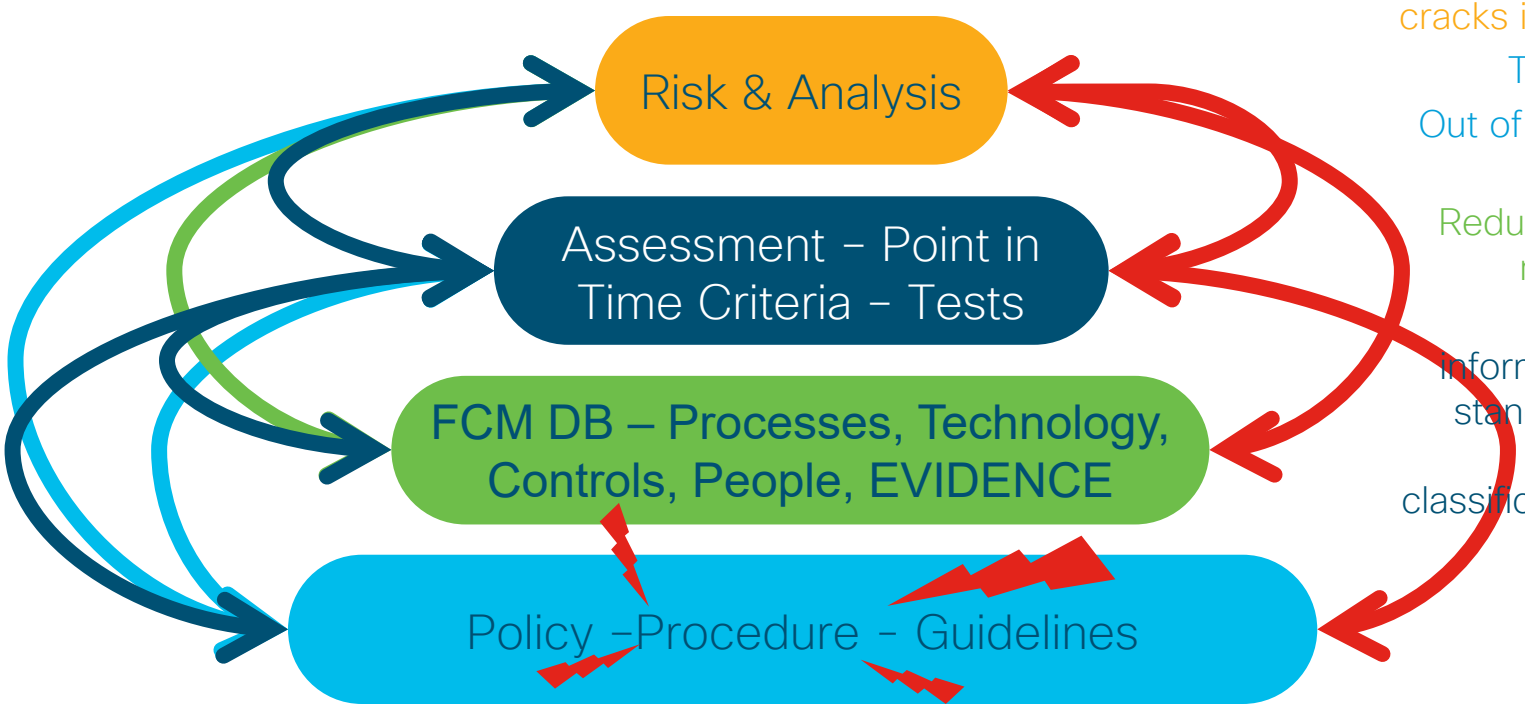
Once mapped to the ISMS, all frameworks add to the overall heat map, identifying areas posing greatest opportunity and weakness. (See ISMS Risk Remediation Management)

Control Assurance Methodology uses Process Steps to assess risk across all standards

FCM Configuration Management DB

All assessment models leverage people, processes, technologies, and product based scope and boundary. **Key requirement is the universal evidence repository.**

Stress on our Foundation is Causing Fault Activity



Here's what's putting cracks in our foundation:

Too many policies

Out of date or incorrect procedures

Redundant efforts and no feedback loop

Wrong level of information per policy, standard, guideline v. SOP affecting classification and use on the document

Lack of evidence mapping

Sample Unified Project Timeline

Phase 1

Understand product compliance committments

Analyse existing controls, Internal Authority to Operate, ISO27, SOC2, FedRamp, etc.

Inventory the outcomes, process & artifacts

Phase 2

Digitize - FCM contains People, Process, Controls, Audits SOC2 – ISO 27 and ATO – ISO27 control level mapping complete, GAP – ISMS Risk Reports,

Native Tagging to Evidence locations and Evidence Mapping

Phase 3

Evidence mapping adoption, Control to Test level mapping, NIST to Authority to Operate – ISO – SOC2 – Unified Risk Analysis, Policy Mapping adoption, Roll Forward Testing Process

Phase 4

Investment in a Platform for shared controls and policy requirement mapping

All compliance models mapped (example GDPR/C5/SecNum)

Optimize organic authority to operate procedure

Phase 5

Internal Assurance Framework published control narrative and common evidence enables Third Party SIG

Controls Assurance Leverages Product Security Assurance

Refined Unified Question Bank ties out all Assessments

Adding compliance assertions is structured with predictable sourcing, allowing for accurate ROI

What's in an FCM?

FCM Content includes regulations and standards frameworks as commonly required in public SaaS based industry. Information requires constant grooming.

FCM Has People, Policies, Assurance Processes, Controls, Tests, Risk Management, Reporting

FCM is PMM level 5, CMM level 1 – it gets us ready to work on a platform. It is not a platform.

FCM Models Cyber Risk Management Content – in a platform like Archer plus UCF content =<100 more

Center for Internet Security Critical Security Controls Version 6.1(v7 req.)

Authority to Operate: ~ATO*

Cloud IT service providers (SecNumCloud)

Cobit 5 © ISACA 2013

Compliance Controls Catalogue (C5)

COSO 2013

Criminal Justice Information Services (CJIS) Security Policy

CSF Framework for Improving Critical Infrastructure Cybersecurity

FFIEC Handbook

FFIEC Cybersecurity Assessment Tool

Cybersecurity Risk MGT Program – Description Criteria © AICPA 2017

General Data Protection Regulation (EU) 2016/679

HIPAA Assessment

HIPAA – HITECH Title 45 C.F.R. § 164

CSF 9 (HITRUST)*

ISO/IEC 27001:2013 €

ISO/IEC 27002:2013 €

ISO/IEC 27002:2017 €

NERC CIP

NIST 800-171 r1

NIST 800-53 r4 (soon r5)

PCI DSS V3.2 Copyright © 2016 VISA

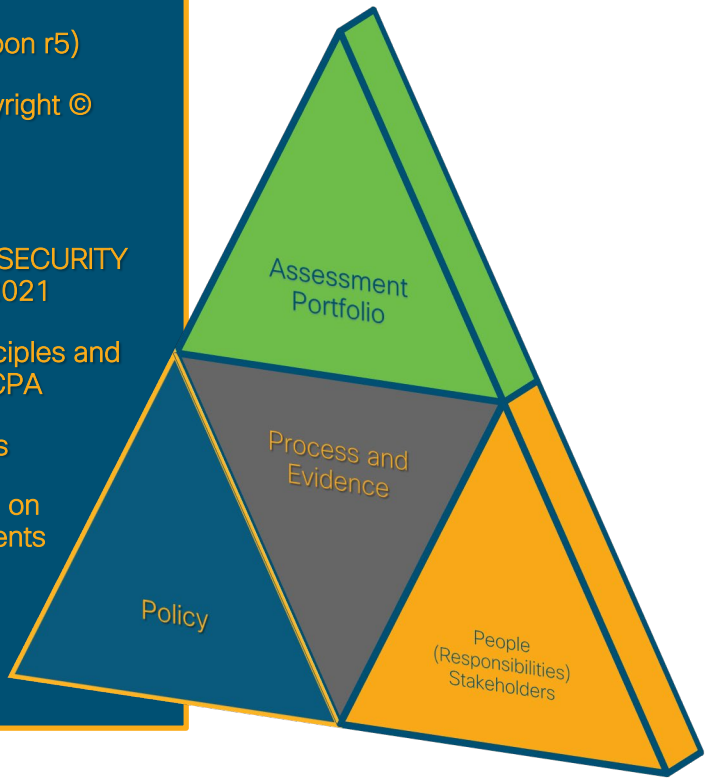
Privacy Shield

NATIONAL CYBER SECURITY STRATEGY 2016-2021

Trust Services Principles and Criteria © 2017 AICPA

UK Cyber Essentials

… sample, depends on company requirements



How does connecting controls, programs, and products make us stronger?

Begin with who we are.

Leverage what we already know.

The Future – Less Time, More Compliance

How do we make this more efficient, quicker, less costly?

Security Best Practices; OWASP, CIS,ENISA, NIST

Unified Process Model, Control Assurance Framework, FCM

Documentation Best Practices Map to Policy Framework

Plan

What processes will we test? What questions will we ask?

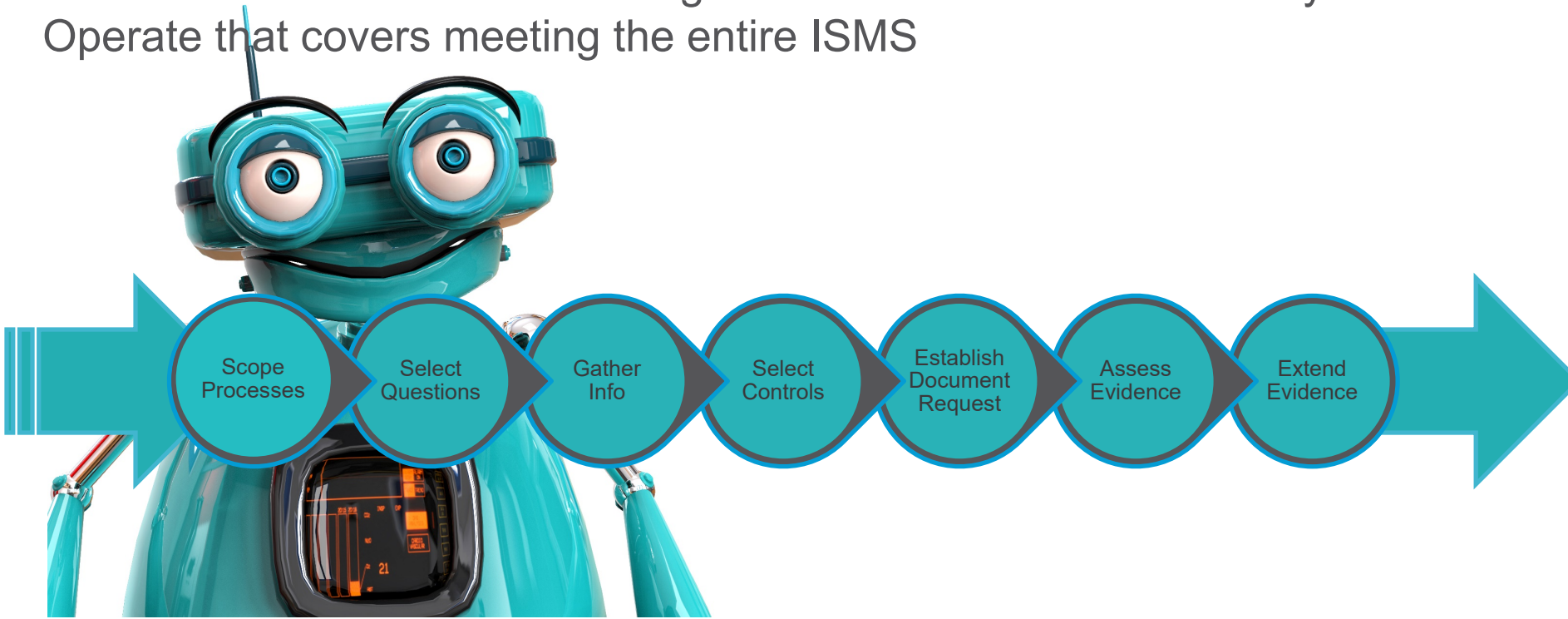
Connect

Focus on Relationship and gathering information

Negotiate

How far can we stretch evidenced processes? To ISO, FedRAMP, SOC 2, ~ATO*, HITRUST, ESCloud Label (C5, SecNum) ?

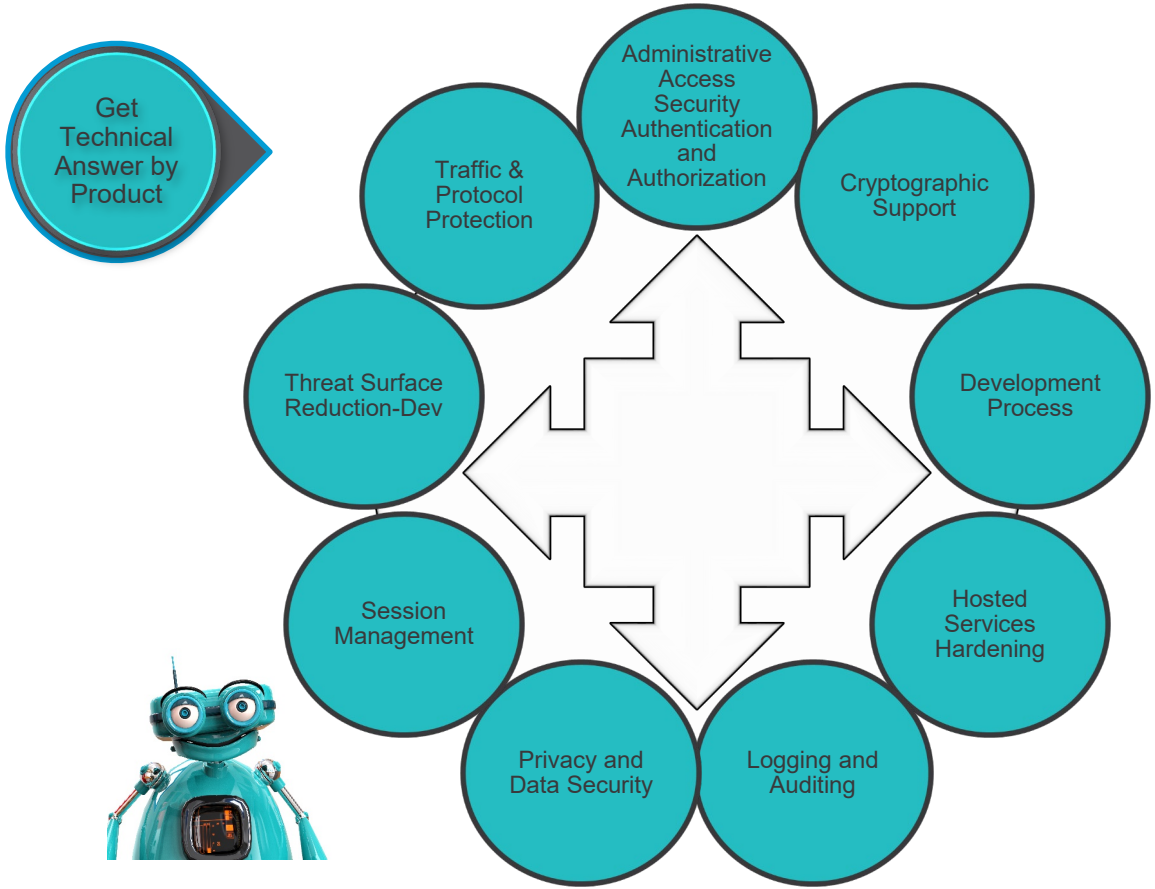
As each Product/Service engages in their Common Control Assurance Framework Information Gathering Process it assures an Authority to Operate that covers meeting the entire ISMS



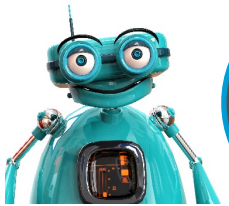
Authorized to Operate goes first

One Button Assurance Framework Leverages Authority to Operate process as the primary source of Unified Compliance information

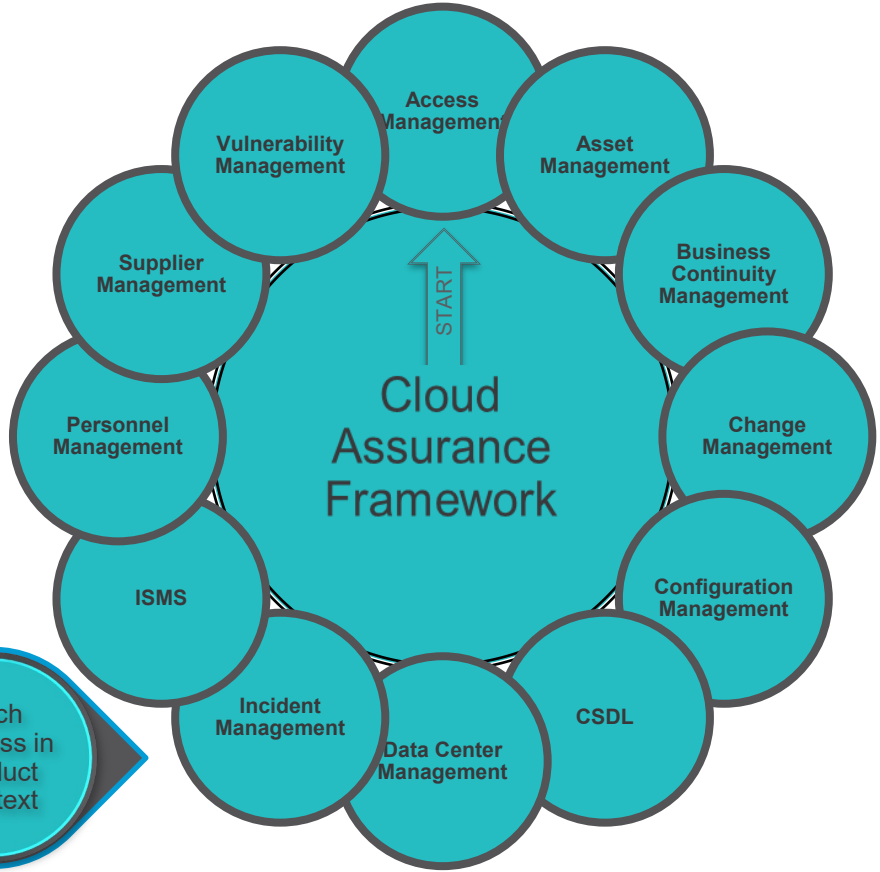
Extract technical answers from Product Security, Target Product & Service



Examines distinct processes against product context
Reduce questions to ten common verifications
Track the evidence



Each Process in Product Context



Questions?