RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SOP-W08

Adaptive & Unified Approach to Risk Management and Compliance via CCF

Vishal Kalro

Manager, Risk Advisory & Assurance Services (RAAS)
Adobe
@awish11

Disclaimer

All the views presented here are my own and not of the organization with which I am employed or was employed with. The material presented here is for educational purpose only and is up to the participant as to how to make best use of it.

Agenda

- Setting The Stage & Reality Check
- Eureka - Adaptive and Unified Approach via. CCF
- Future Is NOW
- Q&A

Setting The Stage & Reality Check

Sightings

Source PWC' s Information Security Breaches Survey 2015

90% of large organizations had a security breach up from 81% year a go

32% of the respondents in 2015 haven't carried out any form of security risk assessment

26% of the respondents don't evaluate how effective their security expenditure is

What comes to your MIND?

IRS sued over data breach that affected 330,000 people

To battle Cyber attacks CEO's need to act more like Military

Hackers drop Zero days opens FireEye fire sale

Airport Computer System Outages Reported Nationwide

Millions Of $$'s Spent On Security & Compliance Fail To Provide A Reasonable Assurance

In Spite Of Networks Being Designed With 99.99 % Availability There Are System Outages & Downtime

In An Event Of A Breach, It Takes Longer Then Expected To Contain The Situation

Source SOPHOS Security Threats Trend 2015

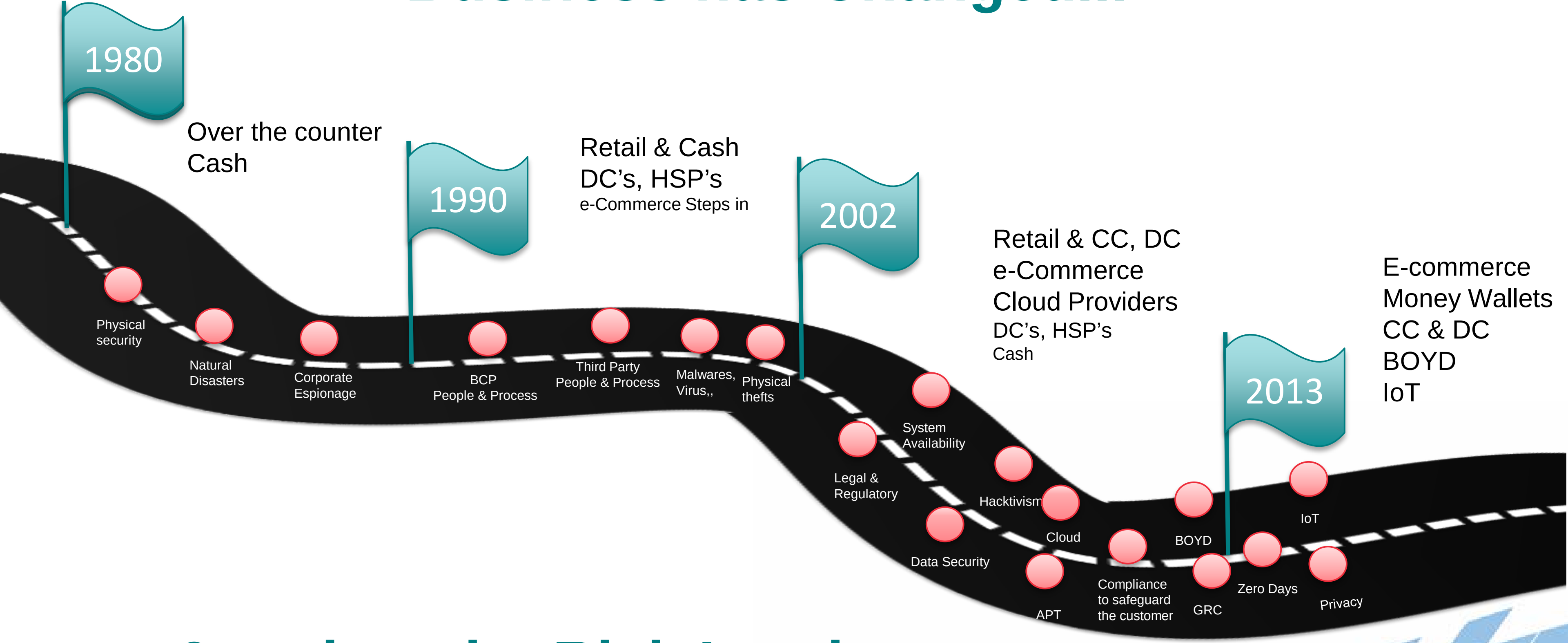
IoT attacks move from PoC to mainstream

More major flaws in widely-used software that had escaped notice by the security industry over **the past 15 years**

Regulatory landscape forces greater disclosure and liability

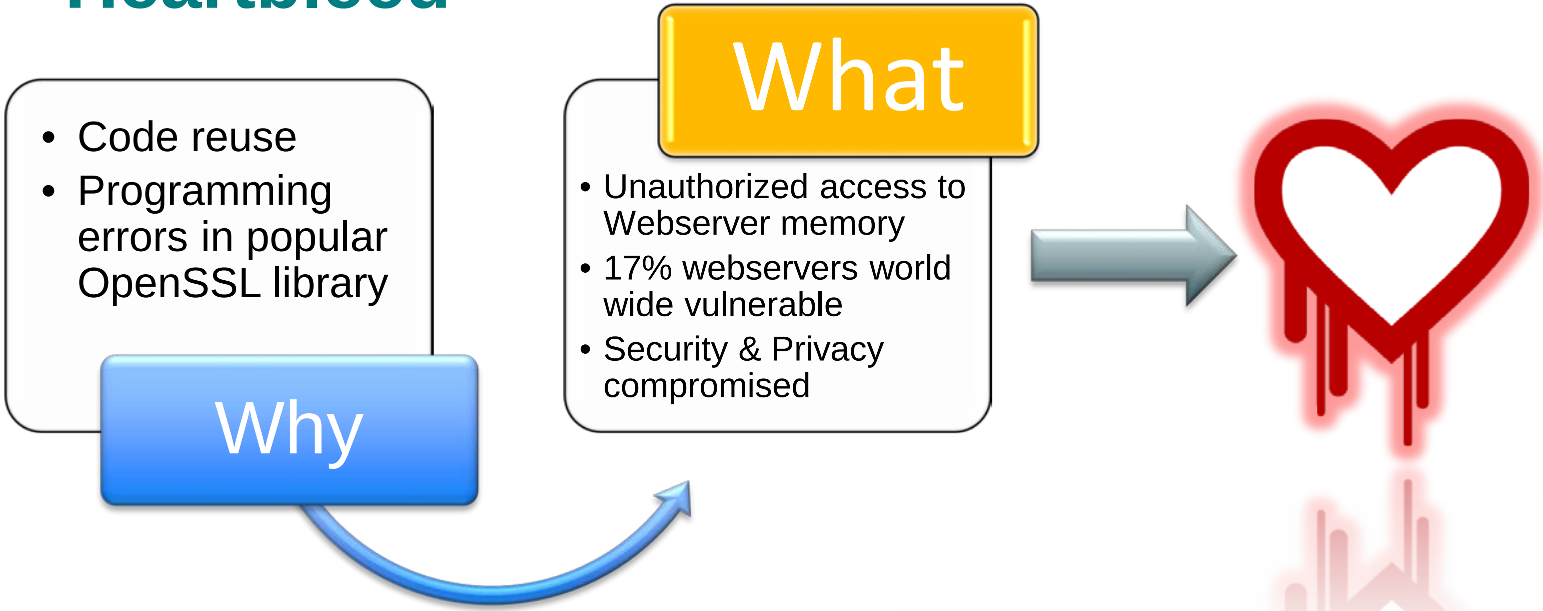
Global skill gap continues to increase, with **incident response** and **education** a key focus

Business has Changed...



...& so has the Risk Landscape

Heartbleed



- Code reuse
- Programming errors in popular OpenSSL library

Why

What

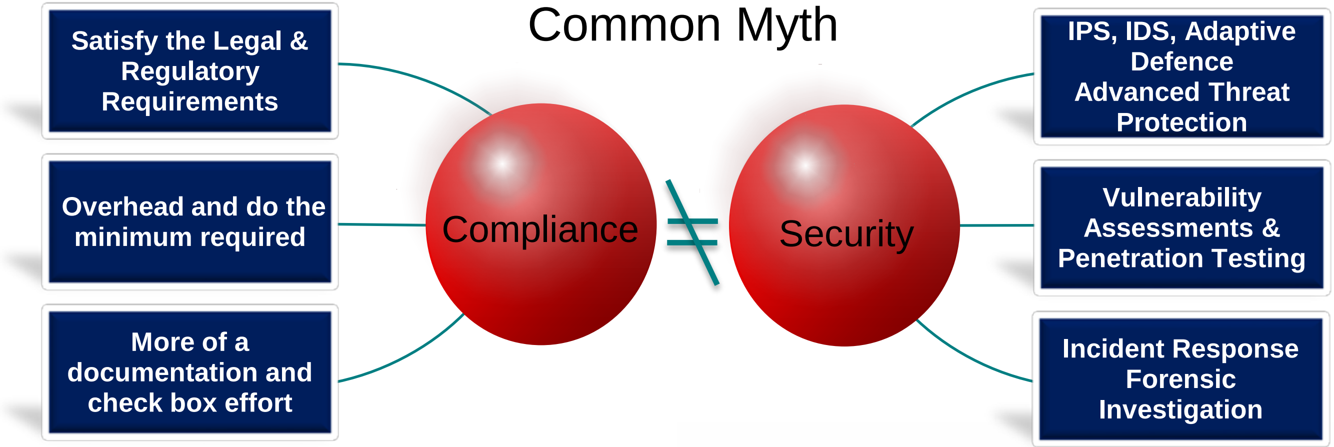
- Unauthorized access to Webserver memory
- 17% webservers world wide vulnerable
- Security & Privacy compromised

Equilibrium –

- A well orchestrated and functional Incident Response process
- Robust asset management program
- Religiously followed system hardening process
- Security should be the soul of SDLC

Reality Check - Compliance vs. Security

Common Myth



Satisfy the Legal & Regulatory Requirements

Overhead and do the minimum required

More of a documentation and check box effort

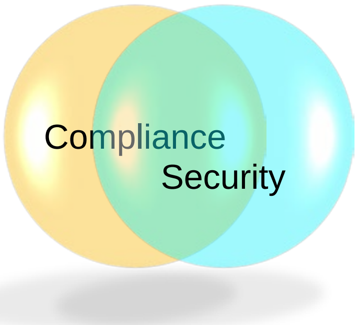
Compliance ≠ Security

IPS, IDS, Adaptive Defence Advanced Threat Protection

Vulnerability Assessments & Penetration Testing

Incident Response Forensic Investigation

Progressive Mind Shift



Compliance as an *enabler, motivator and budget driver* for Security

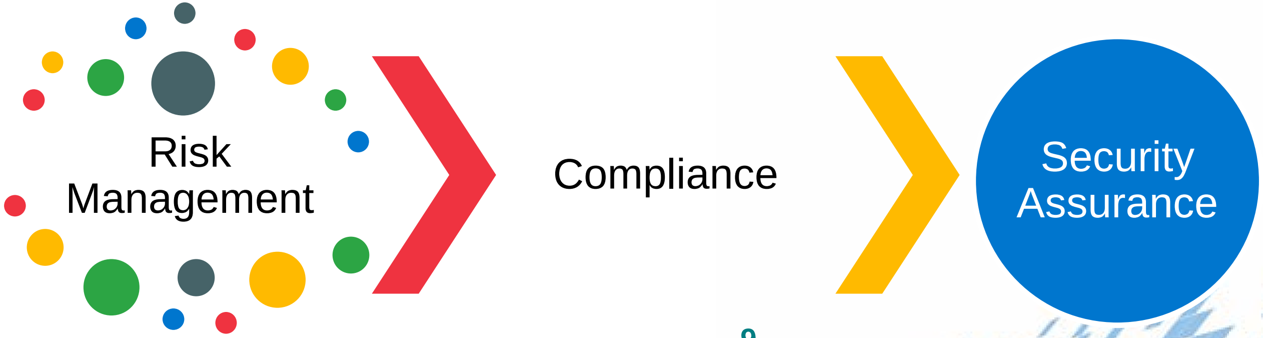
Security best practices lead to *successful Compliance*

All round minimum Security can be achieved by Compliance

Compliance, a *periodic Security health review* by means of *audit*

Security Assurance – Core Competency & Priority

- **Information Security** is a core competency for any service
- Era of **“just trust us”** is over – we need assurance!
- Vendor Priority – **Protecting Customers** and their data
- Security, data privacy & sovereignty are **prerequisites**
- Compliance **accelerates** the Sales and has become a **Competitive Advantage**



Eureka - Adaptive And Unified Approach via. CCF

Man know thyself;
then thou shalt
know the Universe & God

- Pythagoras

Common Control’s Framework (CCF)

10+ Standards,
~1000 Control Requirements (CRs)

~ 200 common controls
across 11 control domains

Risk Assessment

SOC 2 (5 Principles) – 116 CR
Service Organization Controls

ISO 27001 – 26 CRs
International Organization for Standardization

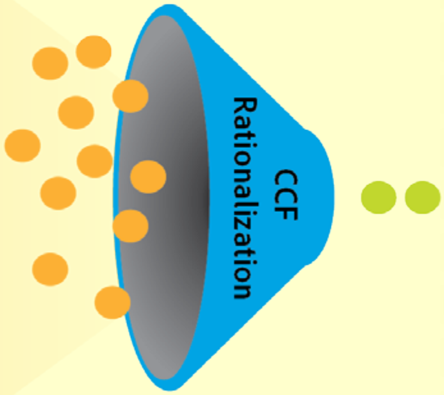
PCI DSS – 247 CRs
Payment Card Industry – Data Security Standard

FedRAMP – 325 CRs
Federal Risk and Authorization Management Program

ISO 27002 – 114 CRs
International Organization for Standardization

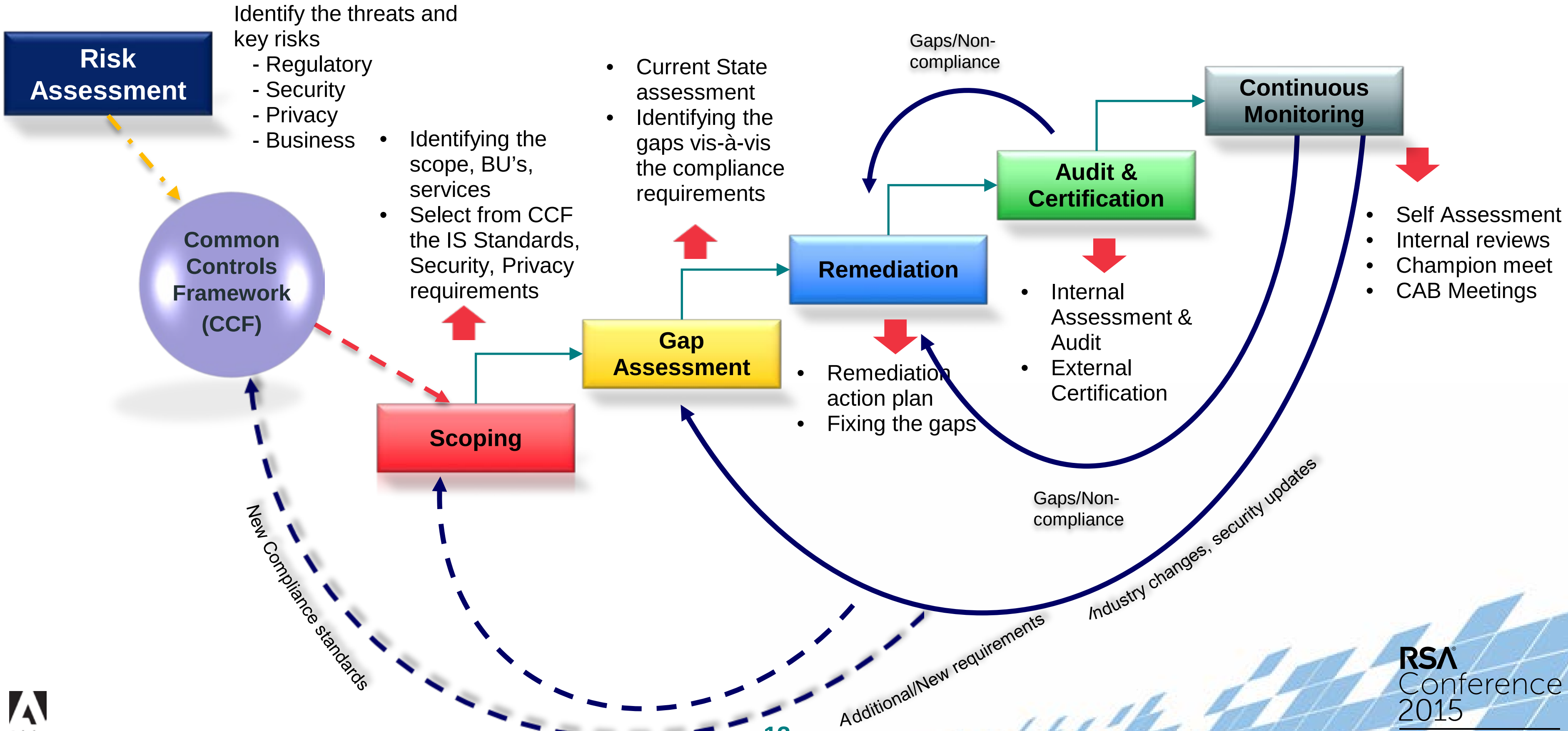
SAFE HARBOR – 7 CRs
Safe Harbor

SOX 404 (IT) – 63 CRs
Sarbanes Oxley 404



Asset Management – 12 Controls
Access Control – 30 Controls
BCM – 10 Controls
Cryptography – 11 Controls
Data Privacy – 10 Controls
Incident Response – 6 Controls
Operations Management – 70 Controls
Physical and Env. Security – 16 Controls
People Resources – 11 Controls
SDLC – 11 Controls
Security Governance – 31 Controls

Roadmap To Assurance via CCF



Risk Assessment

Identify the threats and key risks
- Regulatory
- Security
- Privacy
- Business

Common Controls Framework (CCF)

Scoping

- Identifying the scope, BU's, services
- Select from CCF the IS Standards, Security, Privacy requirements

Gap Assessment

- Current State assessment
- Identifying the gaps vis-à-vis the compliance requirements

Remediation

- Remediation action plan
- Fixing the gaps

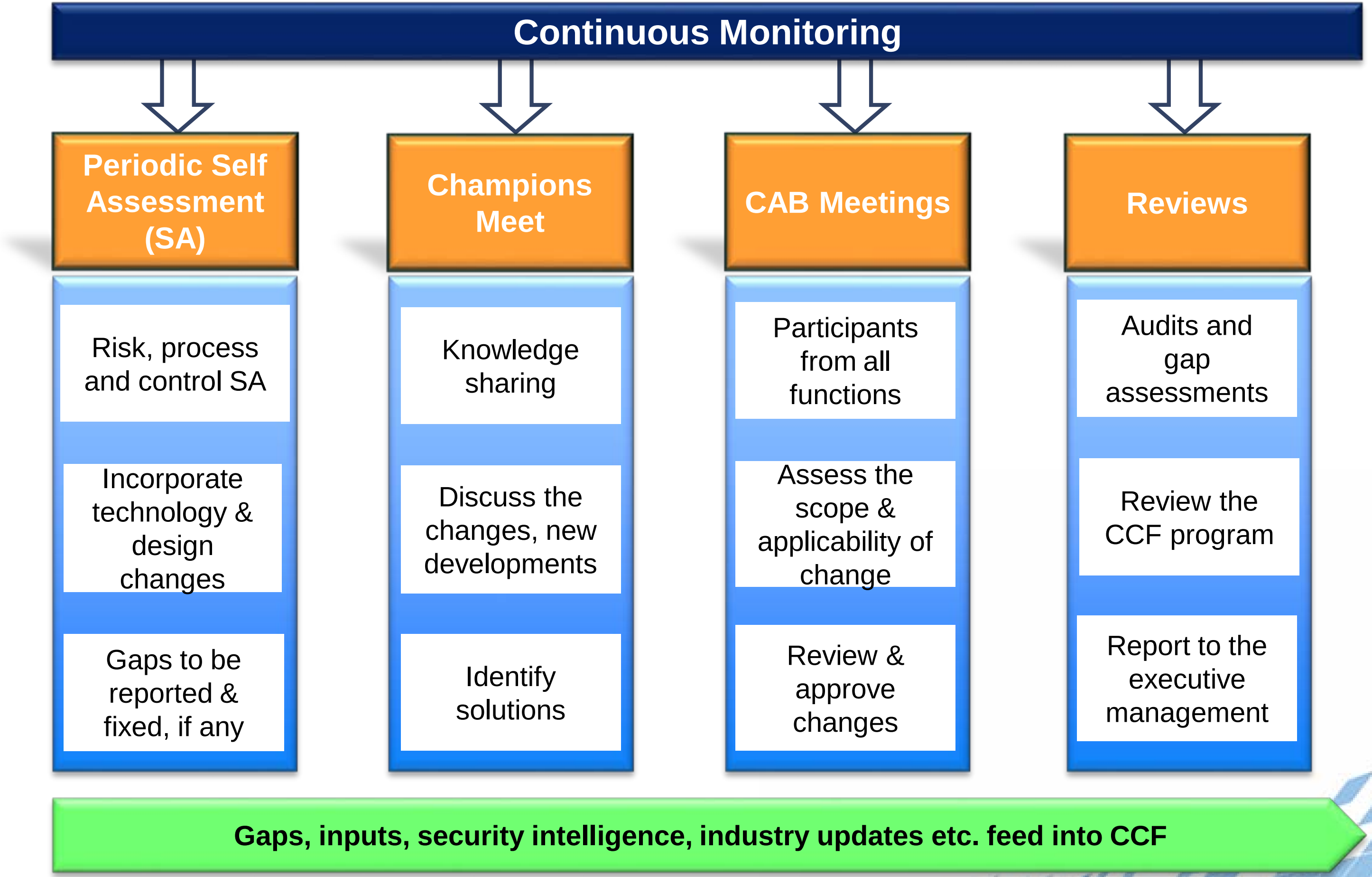
Audit & Certification

- Internal Assessment & Audit
- External Certification

Continuous Monitoring

- Self Assessment
- Internal reviews
- Champion meet
- CAB Meetings

Making CCF An Ongoing Journey



Continuous Monitoring

Periodic Self Assessment (SA)

- Risk, process and control SA
- Incorporate technology & design changes
- Gaps to be reported & fixed, if any

Champions Meet

- Knowledge sharing
- Discuss the changes, new developments
- Identify solutions

CAB Meetings

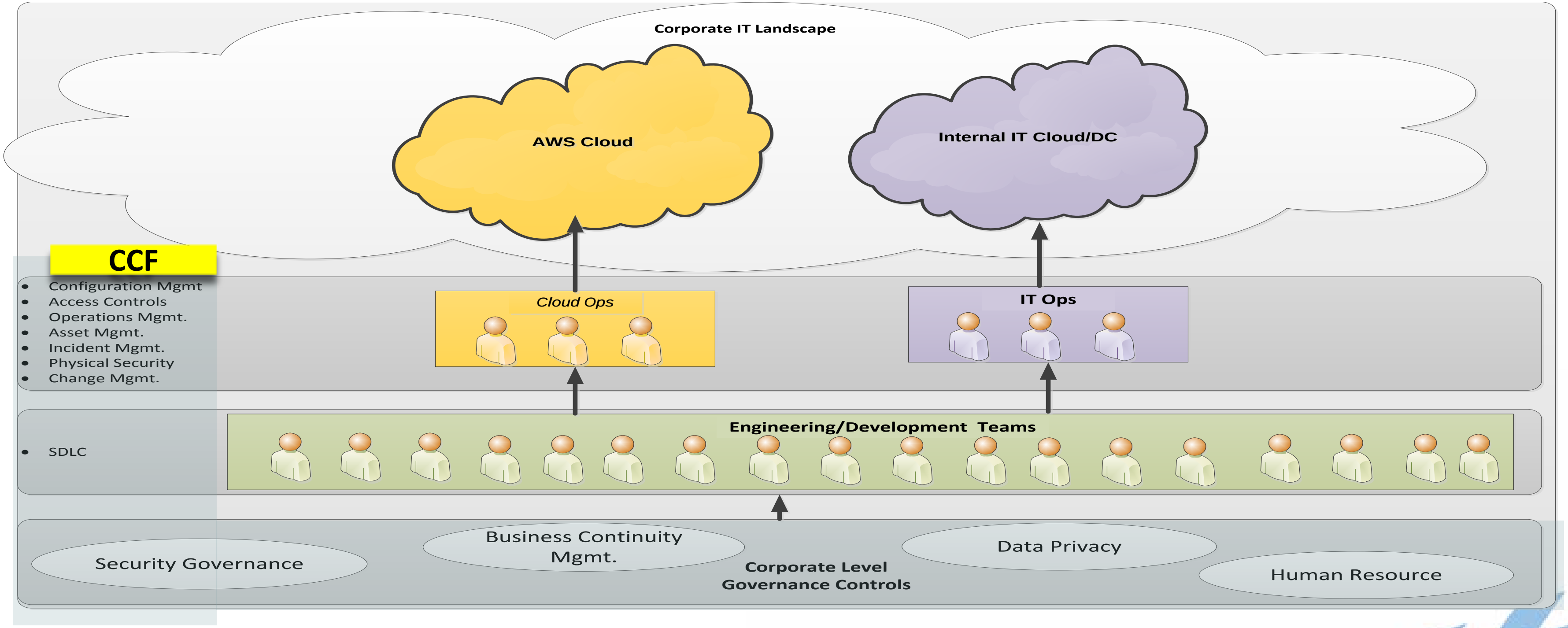
- Participants from all functions
- Assess the scope & applicability of change
- Review & approve changes

Reviews

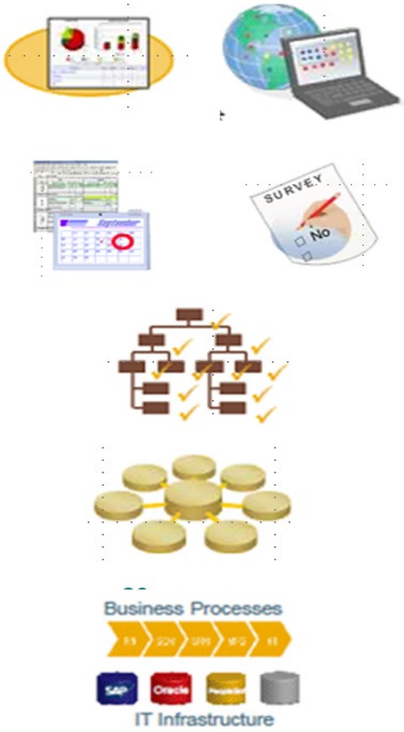
- Audits and gap assessments
- Review the CCF program
- Report to the executive management

Gaps, inputs, security intelligence, industry updates etc. feed into CCF

CCF Conceptual Model



Leverage GRC Technology For Sustainable CCF Compliance



Integrated Compliance Dashboard

Governance, Monitor compliance activity on various levels with real-time reports and dashboards

Standardized Compliance Activity

Automate processes using Assessment and Survey workflow with Issue Escalation

Efficiently Plan, Scope, and Deploy

Leverage integrated program and organizational scoping to efficiently deploy compliance assessments

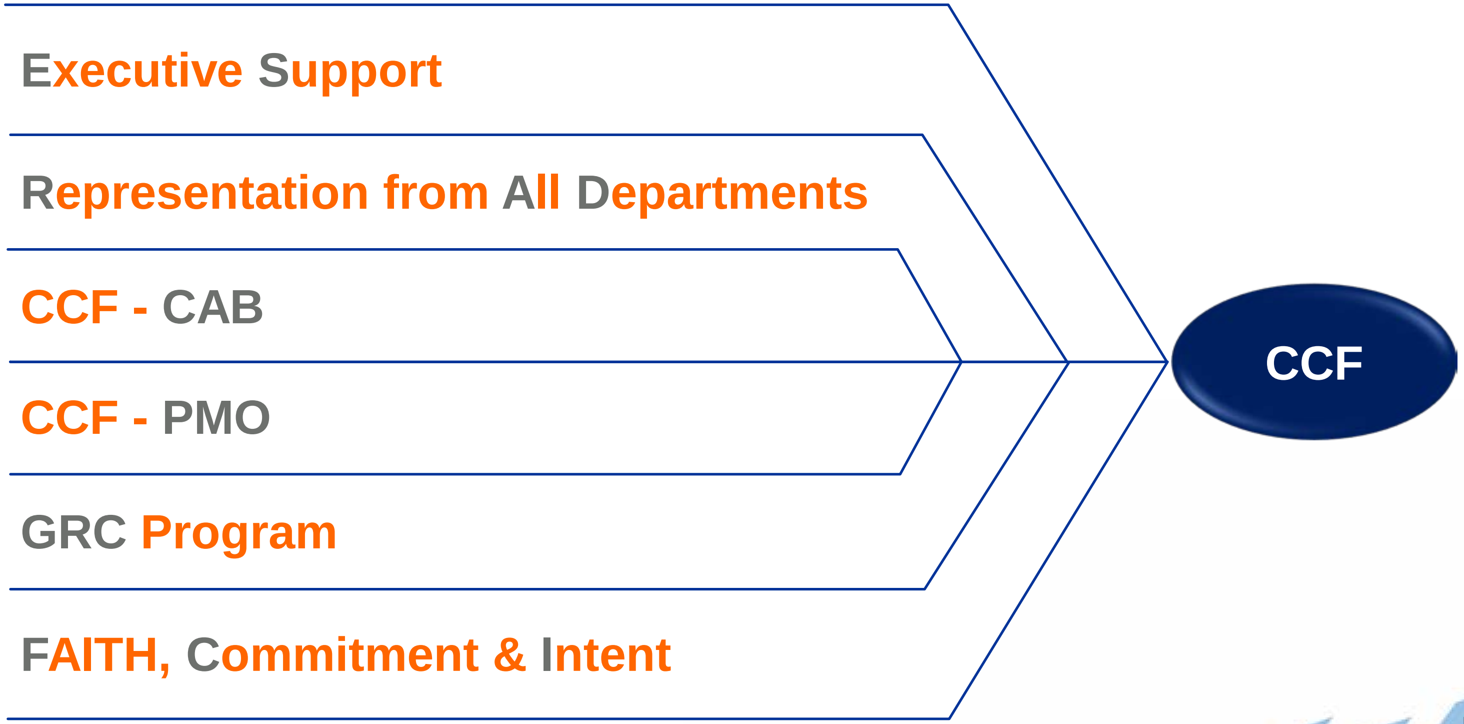
Centralized Program Repository

Integrate compliance program and centrally store files, data, evidence, and results

Automated Controls Monitoring

Automate control monitoring using event-driven, exception-based criteria

Building Blocks of A Successful CCF Program



Executive Support

Representation from All Departments

CCF - CAB

CCF - PMO

GRC Program

FAITH, Commitment & Intent

CCF

Future is Now

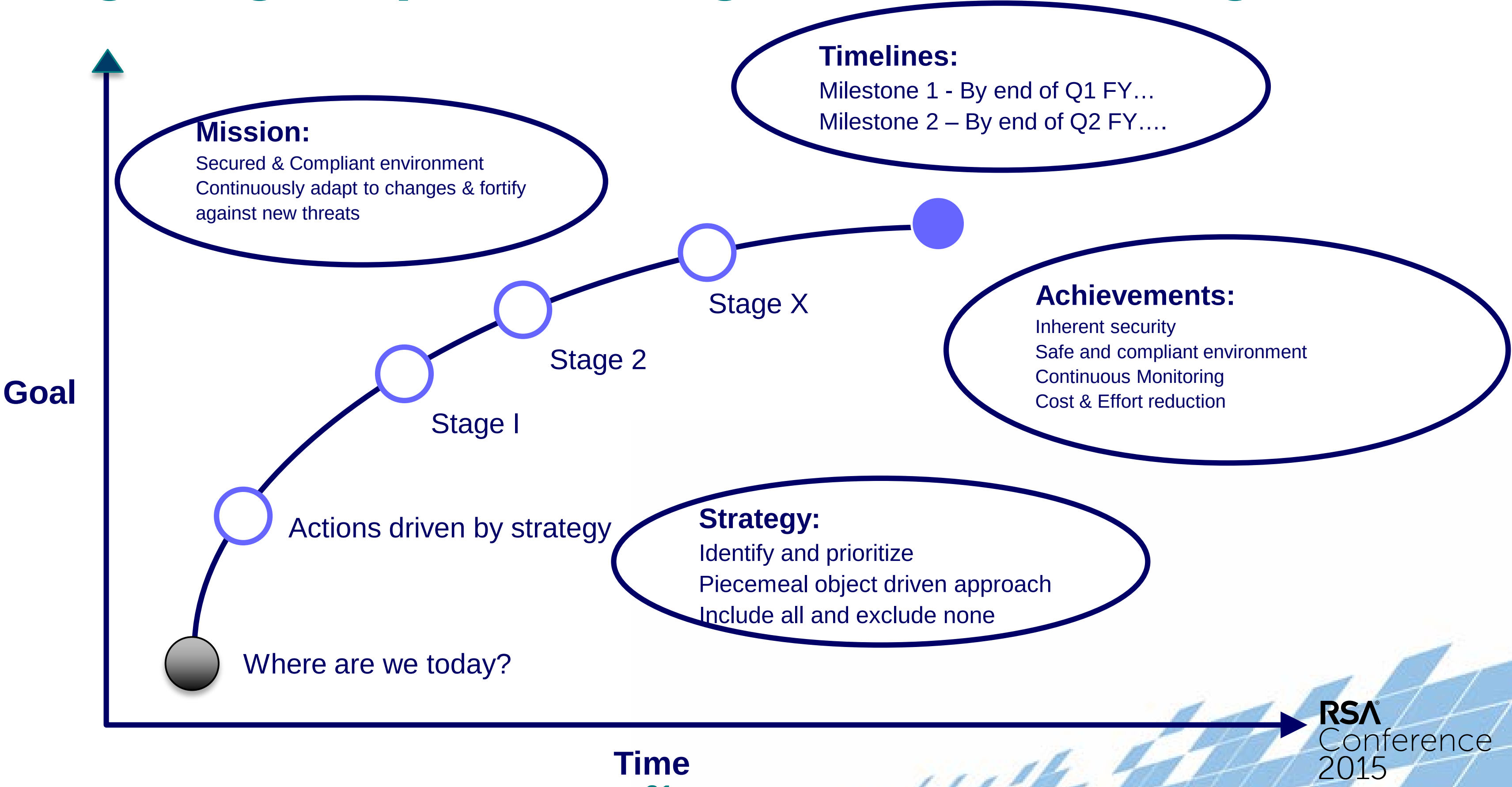
0 Is The Key

- Know Thyself –
  - Develop a high level blueprint of key businesses, IT Operations, different teams, process workflows etc.
    - This Blueprint will be your CCF Conceptual Model
  - Conduct Risk Assessment to identify key risks and threats
  - Make a list of Compliance Standards that your organization needs/wants to comply with – Regulatory, Legal, Customer safeguard, Value proposition etc.
    - Depending upon your business some may be a mandate, some maybe good to have, some may be required by end of next year and so on
    - Put a timeline to each of these requirements

Step After 0

- Develop your own Common Controls Framework (CCF)
  - ❑ Take a piecemeal approach, don’t rush to build it in a day.
  - ❑ Leverage your current Policies, Procedures, Technology & Controls to develop your own CCF.
  - ❑ CCF should cut across all business functions, IT & related operations, teams etc.
  - ❑ Output of Risk Assessment should feed into CCF
  - ❑ Setup a CCF CAB and have representations from all key departments – IT, Legal, Security, Engineering, Business, Marketing & Sales etc.
  - ❑ Make CCF into an intelligent self sustaining program.

Strategizing, Implementing And Continuing



Mission:
Secured & Compliant environment
Continuously adapt to changes & fortify against new threats

Timelines:
Milestone 1 - By end of Q1 FY…
Milestone 2 – By end of Q2 FY….

Where are we today?

Actions driven by strategy

Stage I

Stage 2

Stage X

Achievements:
Inherent security
Safe and compliant environment
Continuous Monitoring
Cost & Effort reduction

Strategy:
Identify and prioritize
Piecemeal object driven approach
Include all and exclude none

Benefits Of A Matured CCF Program

- Secure & Compliant Environment
- Risk Management & Compliance = reasonable Security Assurance
- Self Adaption To Changes And Protection Against New Threats
- Redundant Security Programs And Investments Minimized
- Lot Of $$$$$$’s Saved
- Legal, Regulatory And Compliance Requirements Satisfied
- Edge Over Competitors And Makes A Better Business Proposition

Thank You!

Q&A

Catch me if you want to, at -

vishal.kalro@icloud.com

@awish11