MAINTAINING BUSINESS OBJECTIVES AND LIFTING SECURITY MATURITY

SPEAKERS

Mr James Mouat
APJ Cyber Security Advisor
70 Kent Street, Canberra.
SAP Australia
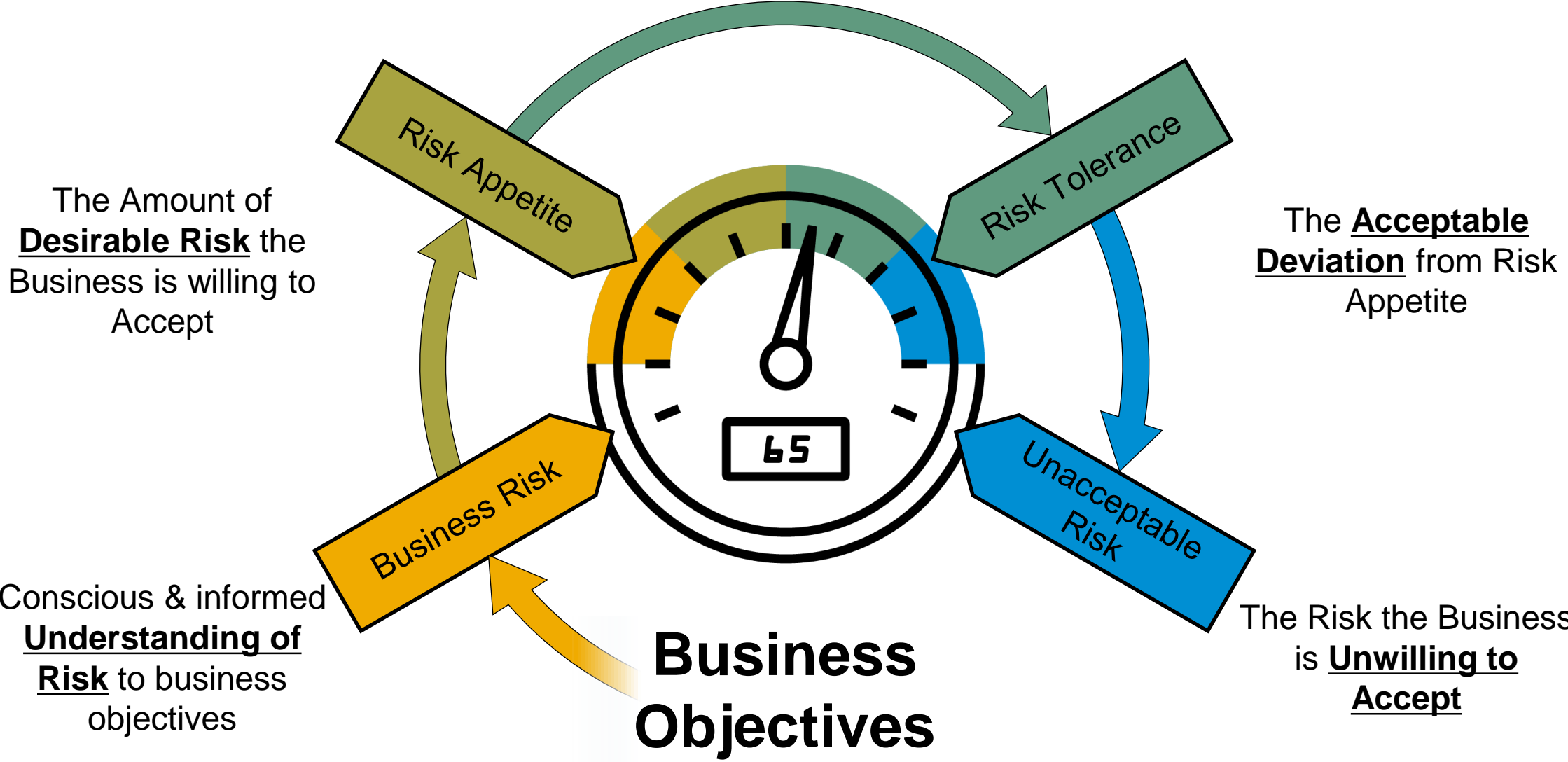
James.Mouat@sap.com

Ms Naomi Benjamin
GVP HXM Technology Architecture
484 St.Kilda Rd Melbourne
SAP Australia

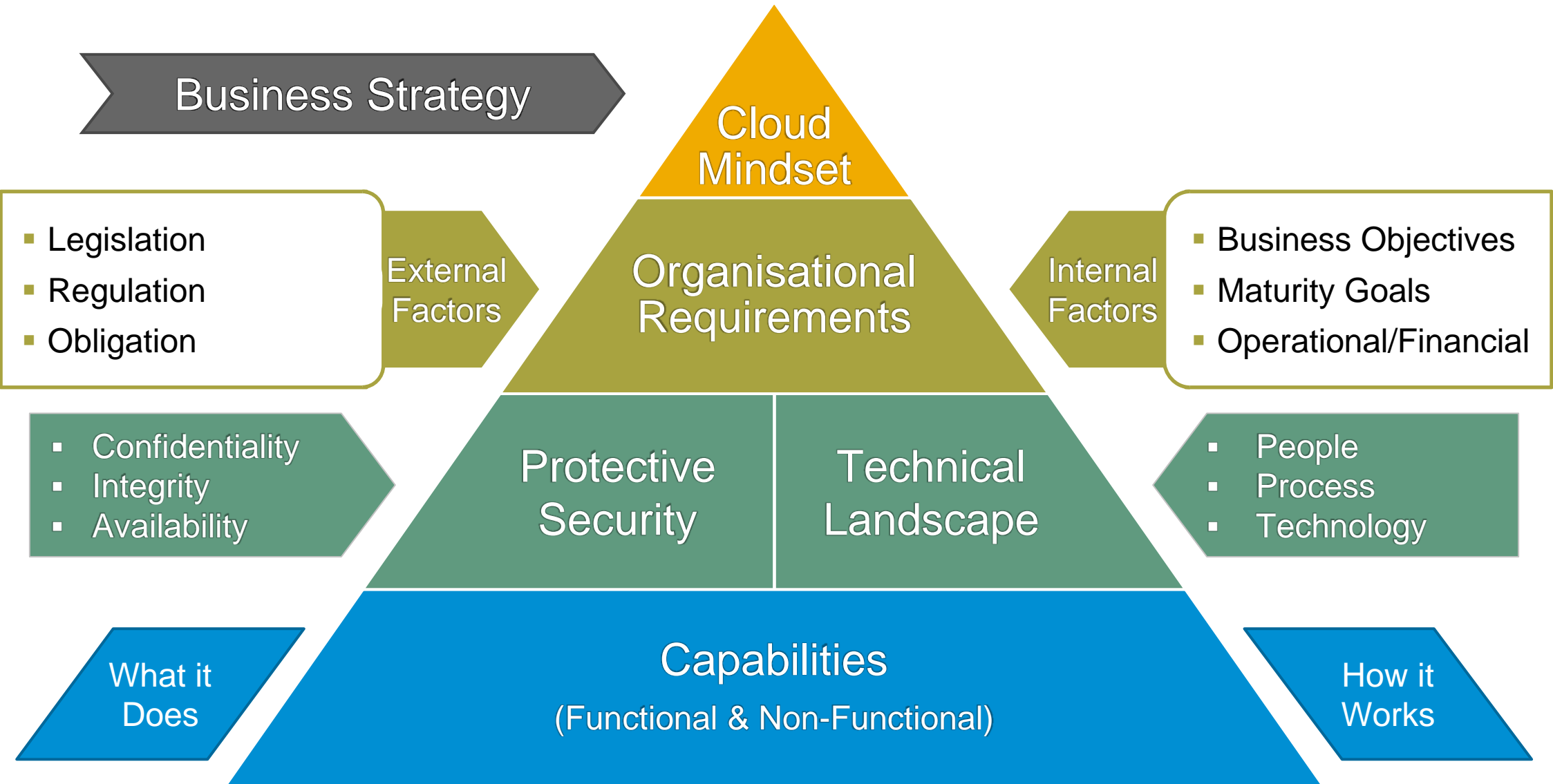Naomi.Benjamin@sap.com

…so what is Risk?

The Amount of **Desirable Risk** the Business is willing to Accept

Risk Appetite

Risk Tolerance

The **Acceptable Deviation** from Risk Appetite

Business Risk

65

Unacceptable Risk

Conscious & informed **Understanding of Risk** to business objectives

Business Objectives

The Risk the Business is **Unwilling to Accept**

My **Desirable Risk** is driving to the speed limit to arrive on time.

Speed Appetite

Adjustable Tolerance

My **Acceptable Deviation** to the speed limit, given identified threats.

Driving Risks

Unacceptable Risk

My **Understanding of current risk** like other Road Users and current Conditions

I'm **Unwilling to Accept** driving without chains in the snow.

Get to my Destination

…what types of Business Risks?

…so what drives Maturity?

…what affects my objectives?

…so what are some New Capabilities?

Cloud Mindset

Release Management Process

What's New Viewer

Preview Instance

QA Instance

Production Instance

Refresh

Sync

Refresh

Sync

Preview Server

Production Server (5 week delay)

60 days prior

Release Summary is available for review

5 Weeks Prior

Release drop in preview instance
Optional features can be reviewed
Relevant approval process

Actual Release Drop

Release drop Production
Approved optional features can be activated

SAP SuccessFactors Data Protection and Privacy

Data Purge
- Configurable customer data retention rules
- Customer approval process before the purge is executed
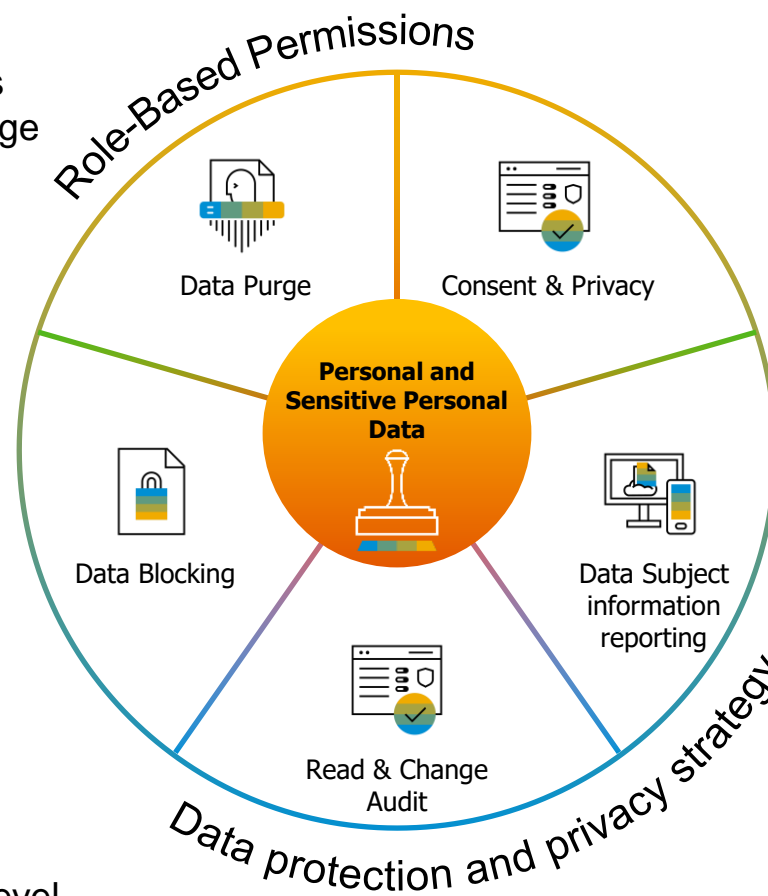- Erasure of personal data, once the full contract is terminated

Data Blocking
- Limit access to data that may need to be retained but blocked from processing for a configurable period
- Obscure sensitive data at the field level and restrict with permissions

Read and Change Audit Logging
With the identification of personal data fields and custom forms you can:
- Track who has accessed sensitive personal data at the record level
- Log changes to personal data at the field level
- Prepare Read and Change audit reports to meet data protection and privacy policy requirements

Role-Based Permissions

Data Purge

Consent & Privacy

Personal and Sensitive Personal Data

Data Blocking

Data Subject information reporting

Read & Change Audit

Data protection and privacy strategy

Consent and Privacy Notice
- Configure and manage consent statements
- Capture and log unambiguous and explicit user consent and acknowledgement of Privacy Notice
- Self-service opt out of email notifications, phone calls where SuccessFactors is controller

Data Subject Information Reporting
- Generate a data subject report containing all the data subjects personal data
- Generate report to inform users about their personal data and logs stored about them
- Data exportable in standard format
- Respond to data access requests
- Allow editing of personal data

General Audit

Generate self-service audit reports

- Audits changes to configuration and data for the platform

- Audit reports for key Role Based Permissions, Proxy Assignment, User Management and Compensation

- Admin Center > Change Audit Reports/Manage Audit Configuration
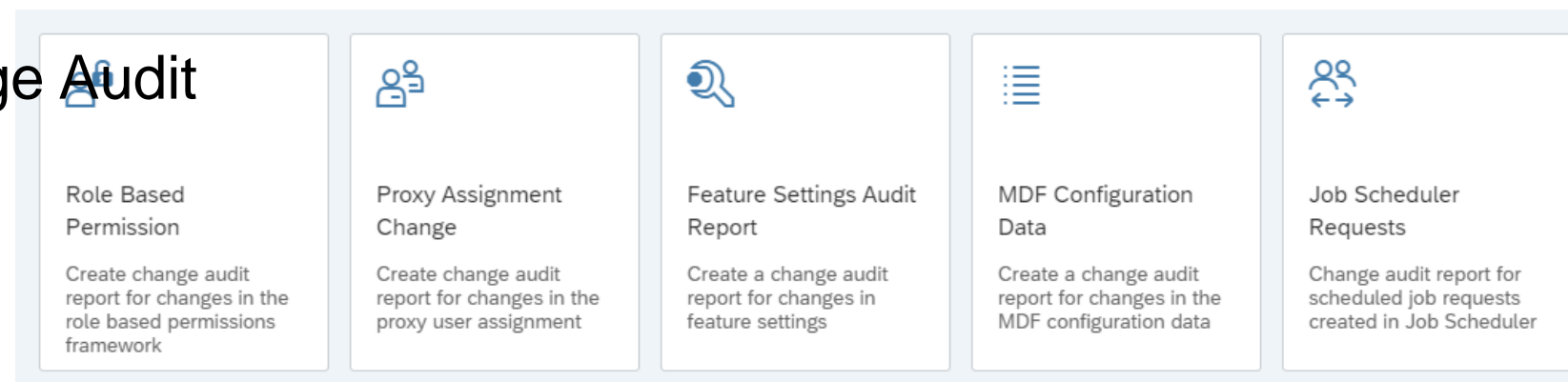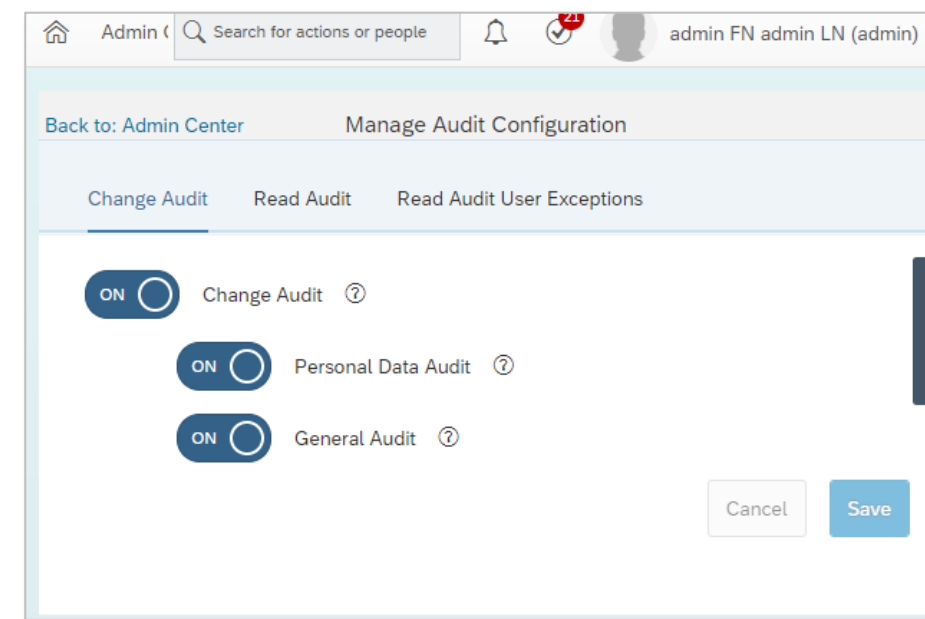
Security measures are audited and confirmed through various Certifications & Attestations
- ISO Certificates
  - ISO27001 Information Security Management System
  - ISO27017 Implementation of cloud specific information security controls
  - ISO27018 Protection of personal data in the cloud
  - TISAX
- FSTEC - Certificate of Conformity
- SOC1 (ISAE3402/SSAE16) Type II
- SOC2 Type II
- C5 Audit Report

Advanced IT Security Architecture
- Multi-tenanted Defence in Depth Architecture
- Data Segregation (Per Customer)
- Security Hardened Systems
- High-Availability & Disaster Recovery

Threat & Vulnerability Management
- Regular Vulnerability Scanning
- Regular Penetration Testing
- Security Patch Management
- 24x7 Security Monitoring Center (Cyber SOC)
- Customer Performed Penetration Testing

Customer data flow control
- European policy General Data Protection Regulation (GDPR)
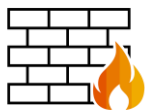
Platform Security
- DDoS Protection at Network Level
- Redundant Load Balancers
- Multi-Tier Architecture
  - Load-Balanced Secure Front End
  - Application Layer
  - Database and Storage
- Firewall Protection at each Tier
- Data in Transit and Data Rest Encryption
- Management & Operations via Jump Host with MFA

Secure Product Development Lifecycle
- Security Planning
- Secure Development
- Security Testing
- Security Validation
- Security Response

Secure Operations
- Asset Management
- Change Management
- Security Incident Management
- Anti Virus & Malware Management
- Backup / Restore Management
- Identity & Access Management
- Security Awareness Training

Physical Security
- Video and Sensor Surveillance
- Access Logging
- Security Guards
- Fire Detection and Extinguishing System
- Uninterruptible Power Supply
- Biometric Access Control in certain Locations

SAP Trust Center
My Trust Center

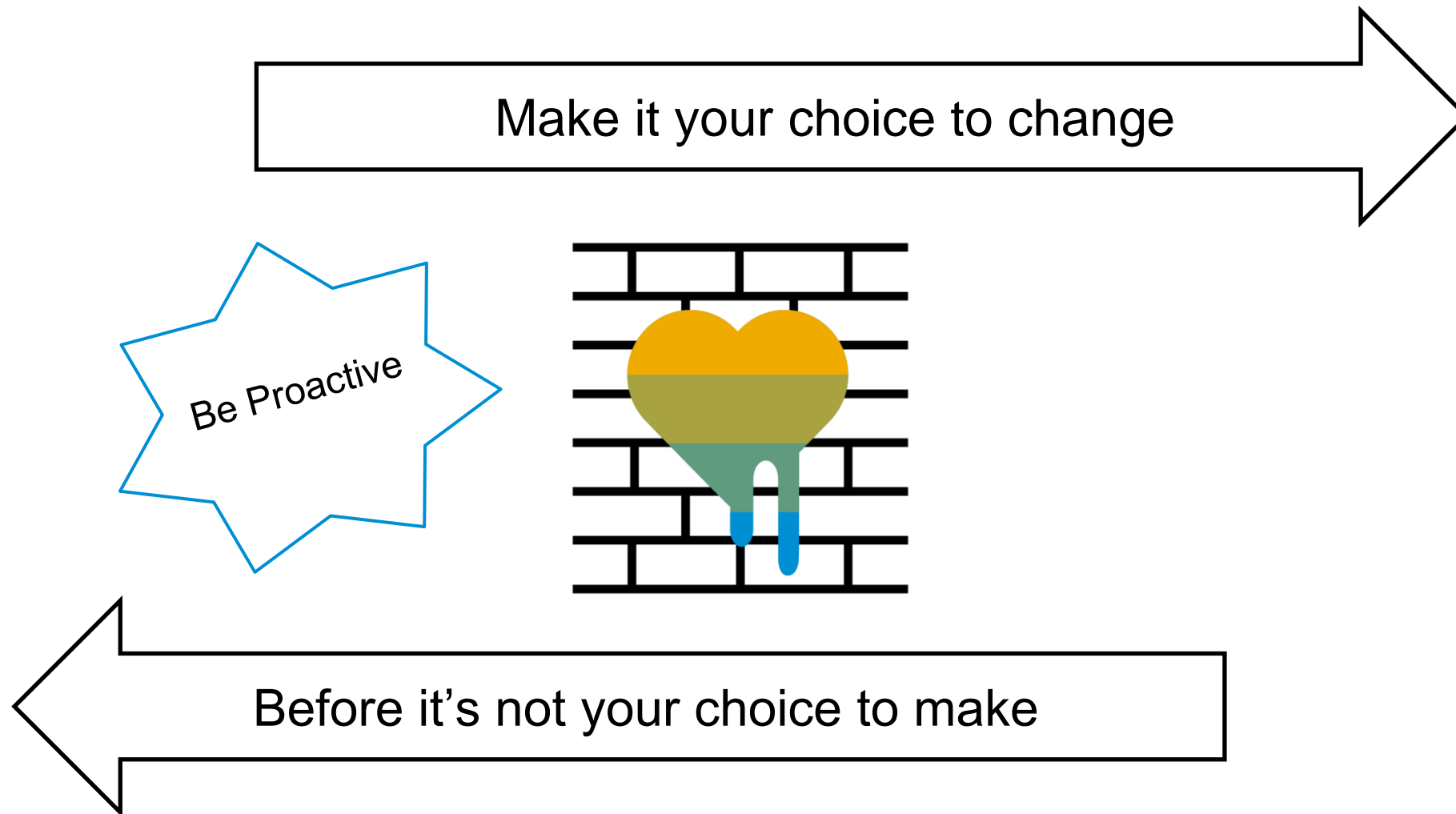https://www.sap.com/sea/about/trust-center.html

The **SAP Trust Center** is a public-facing website designed to provide unified and easy access to trust related content, such as security, privacy, and compliance.
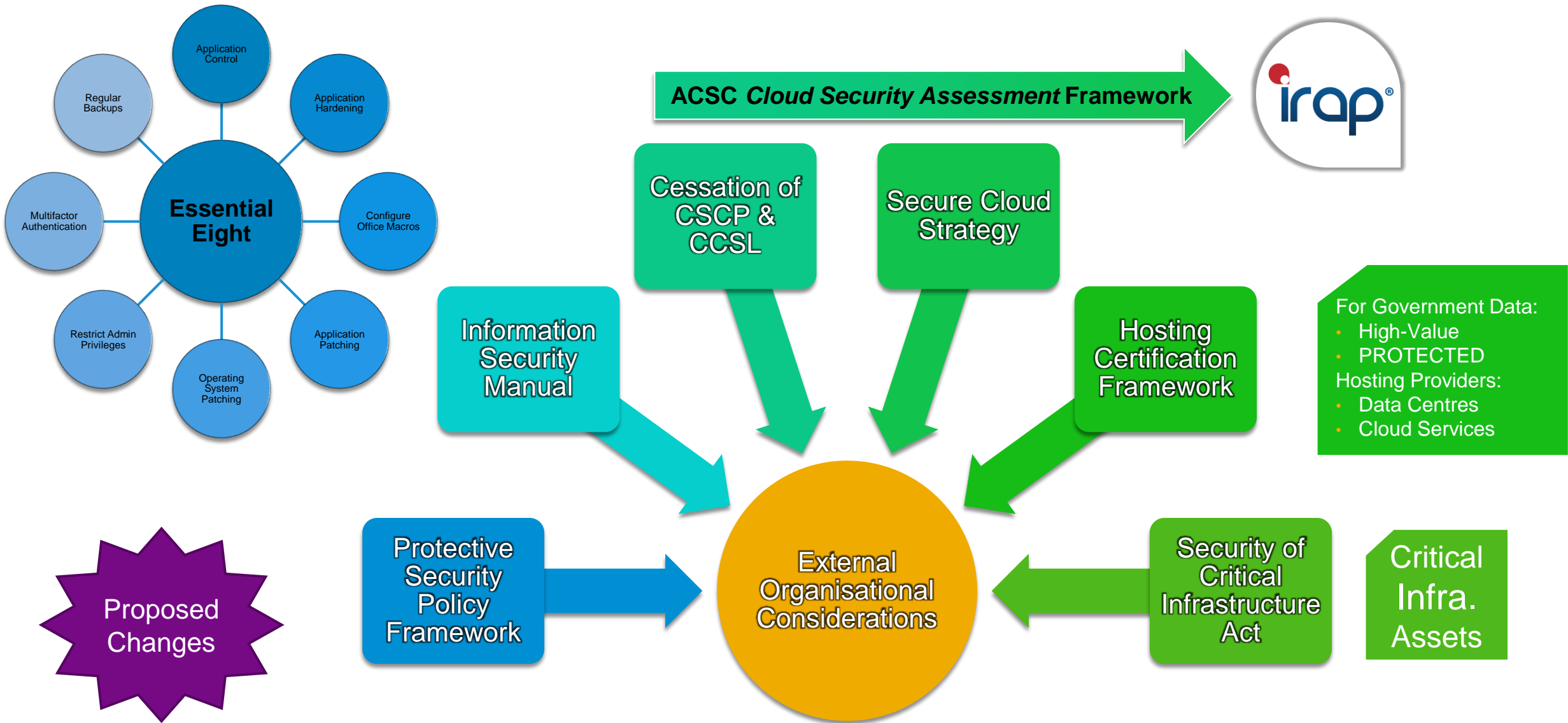- Delivers transparency
- Easy access to SAP trust-related documents, certificates, and contracts
- Users can initiate requests and engage with SAP

Data Privacy & Protection
- Secure Key Management
- Personal Data Breach Notification
- Technical and Organisational Measures
- Data Encryption at Rest and in Transit

Security & Compliance Transparency

…so what should I Consider?

Make it your choice to change

Be Proactive

Before it's not your choice to make

ACSC *Cloud Security Assessment* Framework

Essential Eight
- Application Control
- Application Hardening
- Configure Office Macros
- Application Patching
- Operating System Patching
- Restrict Admin Privileges
- Multifactor Authentication
- Regular Backups

Cessation of CSCP & CCSL

Secure Cloud Strategy

Information Security Manual

Hosting Certification Framework

For Government Data:
- High-Value
- PROTECTED

Hosting Providers:
- Data Centres
- Cloud Services

Protective Security Policy Framework

External Organisational Considerations

Security of Critical Infrastructure Act
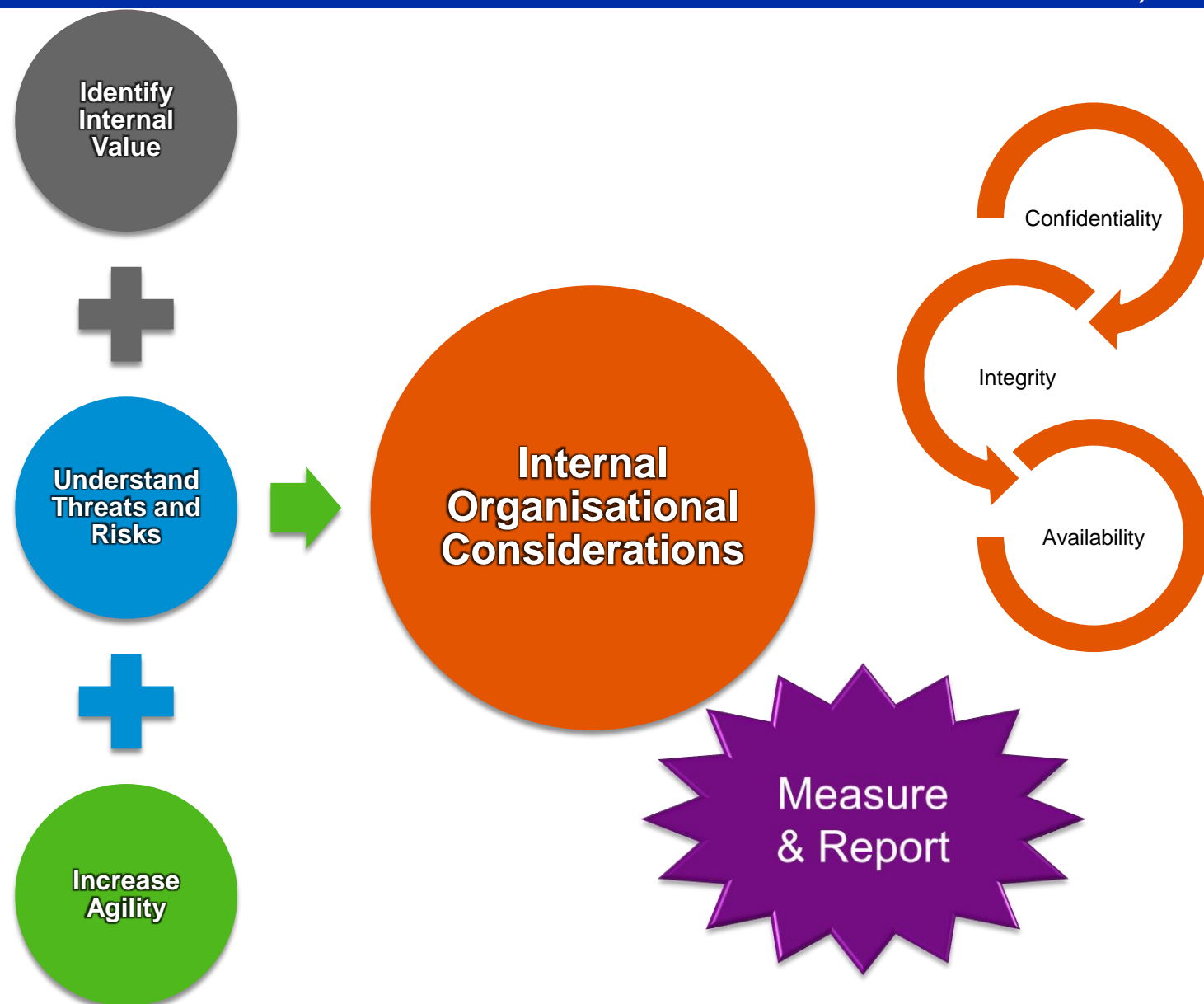
Critical Infra. Assets

Proposed Changes

- ✓ Asset Identification
- ✓ Crown Jewels
- ✓ Damage to Business

- ✓ Current and Future
- ✓ Friend vs Foe
- ✓ Impact to Business

- ✓ Open Communication
- ✓ Transfer Responsibility
- ✓ Shared Accountability

Identify Internal Value

+

Understand Threats and Risks

+

Increase Agility

Internal Organisational Considerations

Confidentiality

Integrity

Availability

Measure & Report

Trust is achieved with Transparency

Security Maturity…

- ...is a Business problem not a Technology Problem

- …must be linked to organisational mission and objectives

- …is gained by effectively managing business risks

- ...is a continual pursuit, not a one-shot exercise

There is no

Business Transformation

without

People Transformation

SAP NOW

Future Proof Your Business

SAVE THE DATE
Date: August 8, 2023
Venue: The Hyatt Regency, Sydney
More details coming soon

Mr James Mouat
APJ Cyber Security Advisor
70 Kent Street, Canberra.
SAP Australia

James.Mouat@sap.com

Ms Naomi Benjamin
GVP HXM Technology Architecture
484 St.Kilda Rd Melbourne
SAP Australia

Naomi.Benjamin@sap.com

- linkedin.com/in/jamesmouat/
- mouat.net.au/ism/

- linkedin.com/in/naomi-benjamin/

#MasteringSAP