Security Culture

Integrity is doing the right thing, even when no one is watching.

– C. S. Lewis

What is Organisational Culture?

Shared values (what is important) and beliefs (how things work) that interact with an organisation’s structures and control systems to produce behavioural norms (the way we do things around here).

Uttal (1983: 66)

So what is Security Culture?

Security culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel within the organization. Security should be everyone’s responsibility - from the ground up and top-down.

(ICAO, 2017)

So what is Security Culture?

Effective security culture is about:

- Recognising that effective security is critical to business success;
- Establishing an appreciation of positive security practices among employees;
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or burdensome expense.

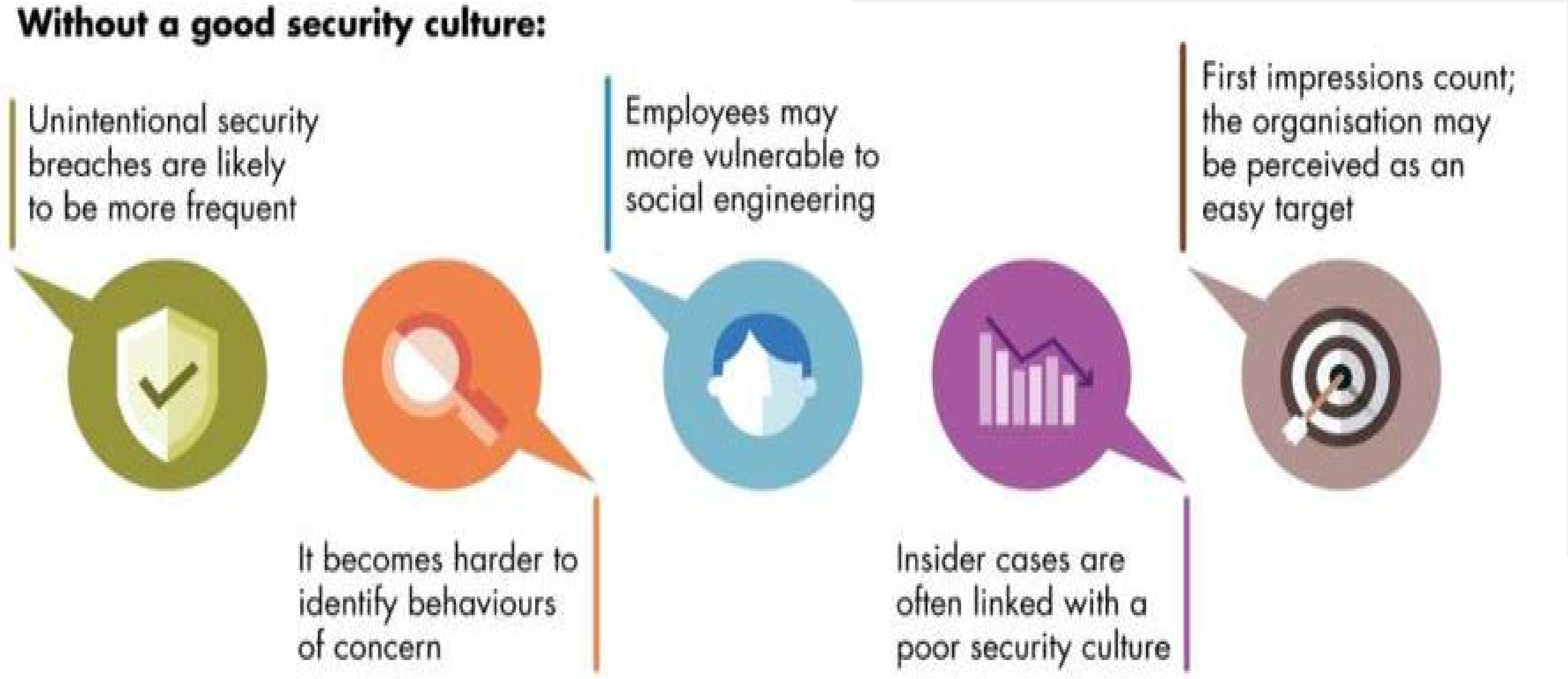
Perception of security

‘Security is everyone's responsibility’ is not just a reminder of individual accountability- its about how security is regarded in an organisation

A Classic Example

- Cleaner who worked for NASA in late 1960s sweeping floors in Cape Canaveral;
- Asked by auditor what his role was in NASA;
- Replied that it was “to put a man on the moon”;
- Spoke volumes about the culture within NASA;
- All play an important role in delivering an organisation’s Key Performance Indicators.

Why is security culture important?



Without a good security culture:

Unintentional security breaches are likely to be more frequent

It becomes harder to identify behaviours of concern

Employees may more vulnerable to social engineering

Insider cases are often linked with a poor security culture

First impressions count; the organisation may be perceived as an easy target

Security Culture – Essential components

- Positive Work Environment
- Training
- Leadership
- Understanding the Threat
- Vigilance
- Reporting Systems
- Incident Response
- Information Security
- Measures of Effectiveness

Positive Work Environment

A work environment which drives and facilitates a positive security culture.

Staff who know exactly what security behaviours are expected of them and who confidently and willingly demonstrate the behaviours.

An organised, systematic approach to managing security which embeds security management into the day-today activities of the organisation and its people.

Positive Work Environment

- Clear and consistent: policy, processes, systems and procedures
- Equipment, space and resources
- Prompts
- Suggestions box
- Targeted communications plan
- Performance appraisals
- Thank you messages
- Security Management System (SeMS)

Training

Staff who have the knowledge, skills and capability to practice good security.

Training

- Induction training
- Refresher training
- Continuous learning activity

Leadership

An environment where managers and leaders, including those at the highest level, lead by example and support their staff in implementing good security.

Leadership

- Leadership briefings
- Example behaviour
- Patience and understanding
- Thank you messages
- Involvement in security awareness events and staff briefings

Understanding the Threat

All staff understand the nature of the threats they and their organisation face

Understanding the Threat

- Targeted threat briefs
- Reminder briefs
- Verbal updates

Vigilance

All staff feel able to challenge those who are not complying with security policy and procedures.

All staff and visitors pay attention to their surroundings when at the airport and know what unusual or suspicious behaviour looks like.

Vigilance

- Repetition
- Reminder briefs
- Visitor briefing notes
- Posters + signage
- Regular security campaigns

Reporting Systems

Security breaches and occurrences are reported swiftly and correctly. Staff do not feel as though they are ‘telling tales’ when reporting an incident.

Reporting Systems

- Just culture reporting system
- Induction training on reporting of breaches
- Rewards/thank you

Reporting Systems

- Indemnity again disciplinary proceedings;
- Confidentiality or de-identification;
- Separation of agency collecting the data from those with authority to impose sanctions;
- Feedback to the reporting community and
- Ease of reporting.

Incident Response

All staff know how to respond and who to contact in the event of an incident

Incident Response

- Wallet cards
- Regular table top exercises and drills

Information Security

Sensitive information is stored, transmitted and disposed of securely and is shared only with those who need to know.

Lost/stolen items such as laptops, phones or papers are reported immediately.

Information Security

- Induction training
- Policy + procedures
- Good cyber practice
- Reminder briefs
- Wallet cards/ intranet quick reference page

Measures of Effectiveness

Improvements in security culture are being made.

Measures of Effectiveness

- Breach records
- Inspection results
- Staff surveys + focus groups

Audience

- Passenger
- Security Staff
- Management
- Senior Management
- Non-security staff
- Contractors

- Public (non-passengers)
- Retailers
- Suppliers
- Enforcement Agencies
- Regulators

Get curious

Health

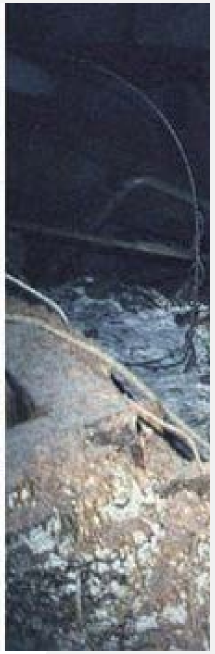
Nuclear

Medical

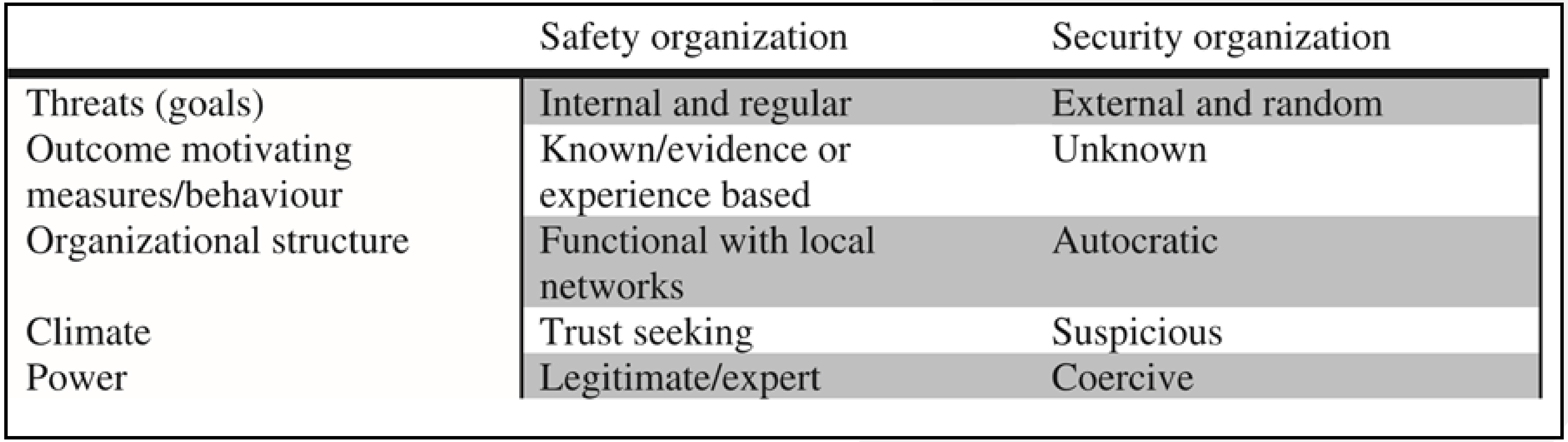
Aviation Safety

Oil & Gas

History

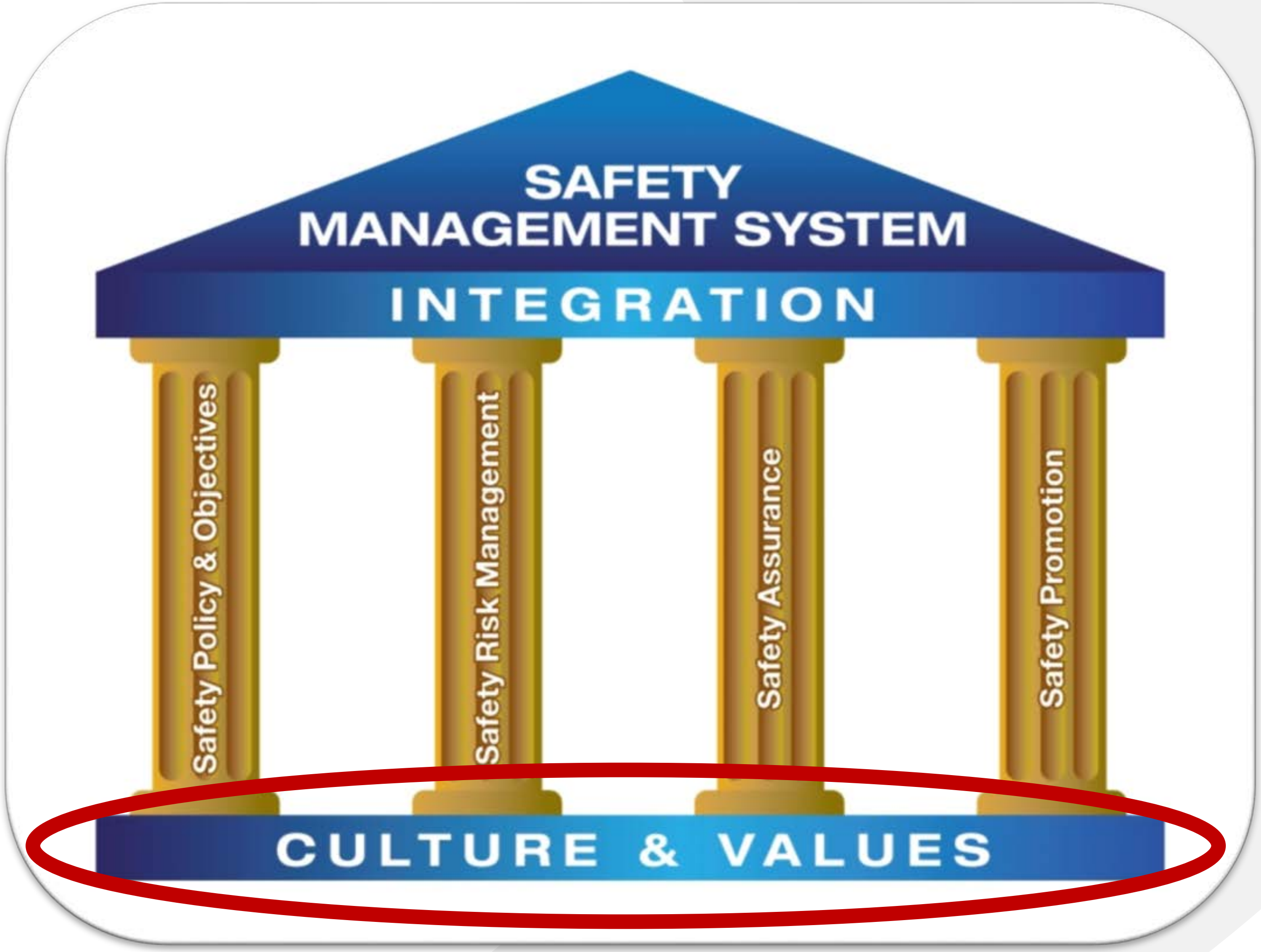


Security and Safety

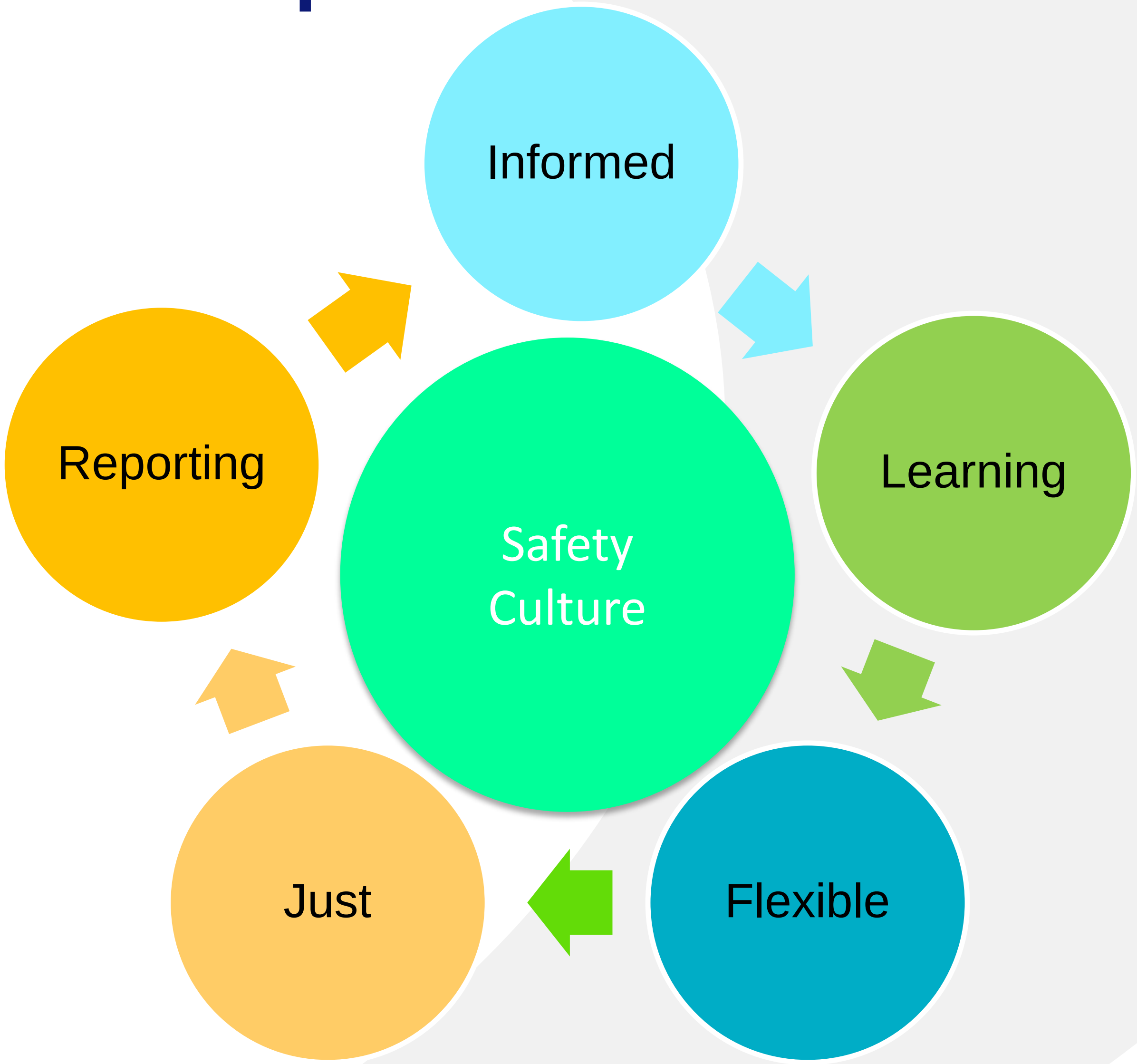


	Safety organization	Security organization
Threats (goals)	Internal and regular	External and random
Outcome motivating measures/behaviour	Known/evidence or experience based	Unknown
Organizational structure	Functional with local networks	Autocratic
Climate	Trust seeking	Suspicious
Power	Legitimate/expert	Coercive

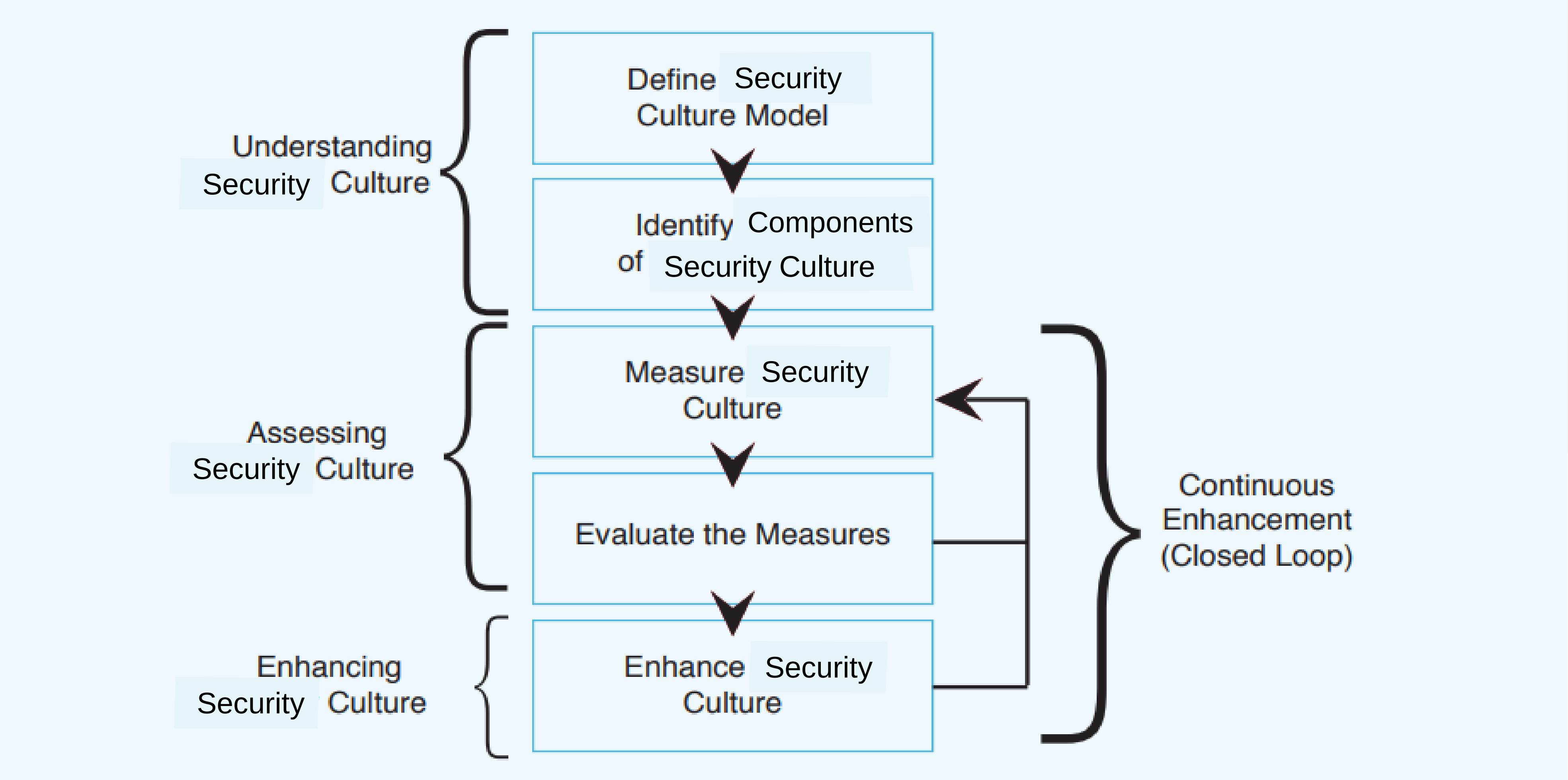
Aviation Safety pillars



Safety Culture components



A Security Culture Model?


Understanding Security Culture
Assessing Security Culture
Enhancing Security Culture
Define Security Culture Model
Identify Components of Security Culture
Measure Security Culture
Evaluate the Measures
Enhance Security Culture
Continuous Enhancement (Closed Loop)

More information

caainternational.com

ICAO YOSC

Kevin.sawyer@caa.co.uk