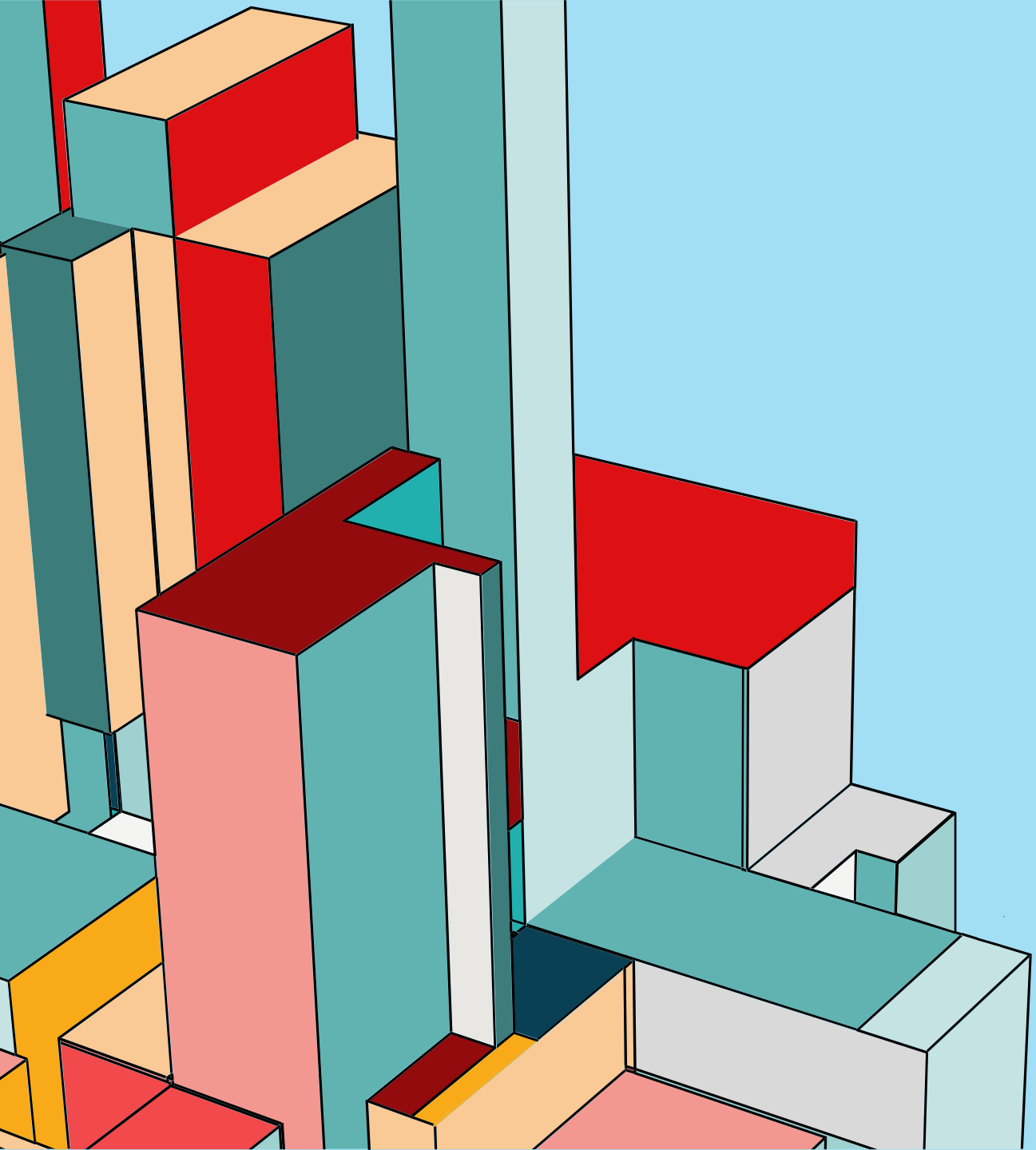


Not too heavy, not too light

Getting your cyber security architecture *just right*

/whois @beLarge

- Principal OT Cyber Security Architect and Chief Evangelist at Secolve
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- Chartered Engineer and Registered Professional Engineer of Queensland (RPEQ)
- Lead of the AISA Security Architecture Special Interest Group (SecARCH SIG) and Deputy Chair of the Queensland Branch of AISA
- Bach Eng (Telecomms) QUT First Class Honours and
  Master Business (Applied Finance) with Distinction QUT

SABSA FOUNDATION LEVEL SCF

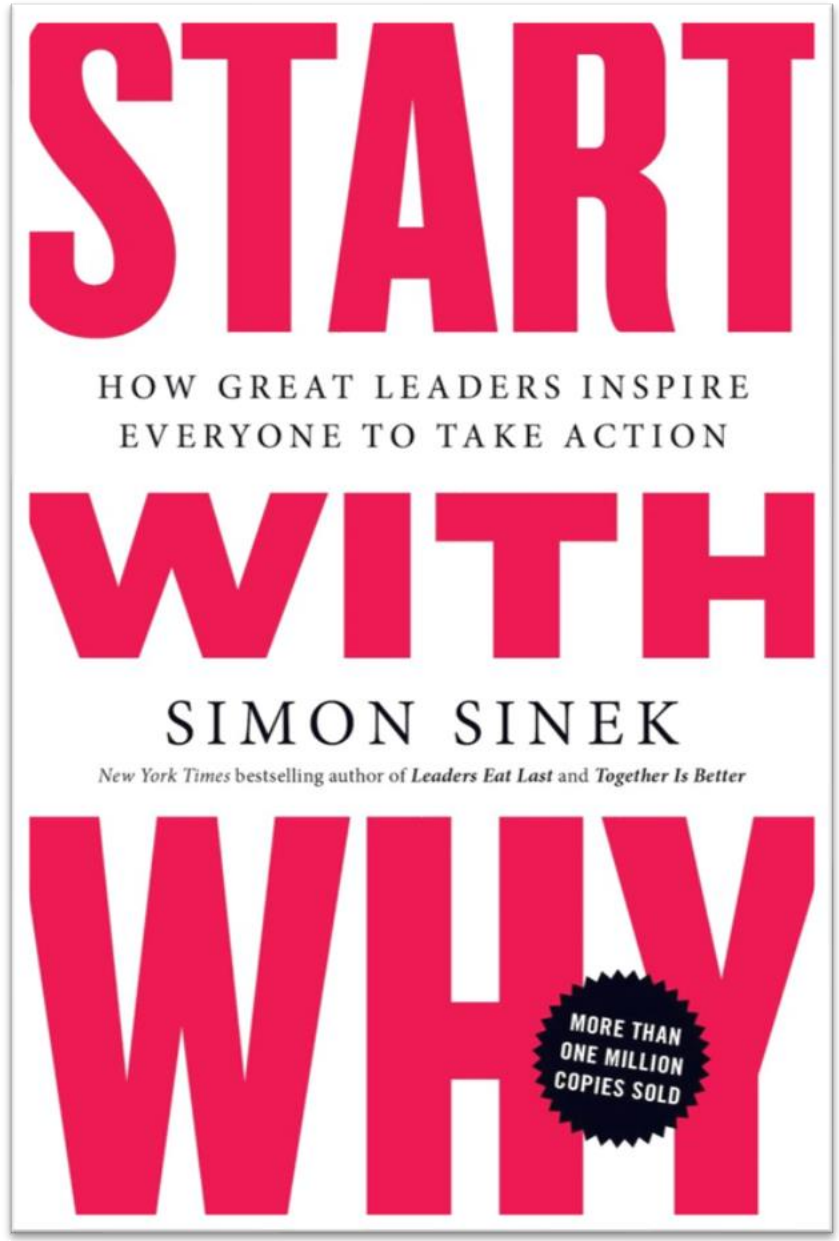
GIAC SECURITY OPERATIONS MANAGER GSOM

GIAC INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

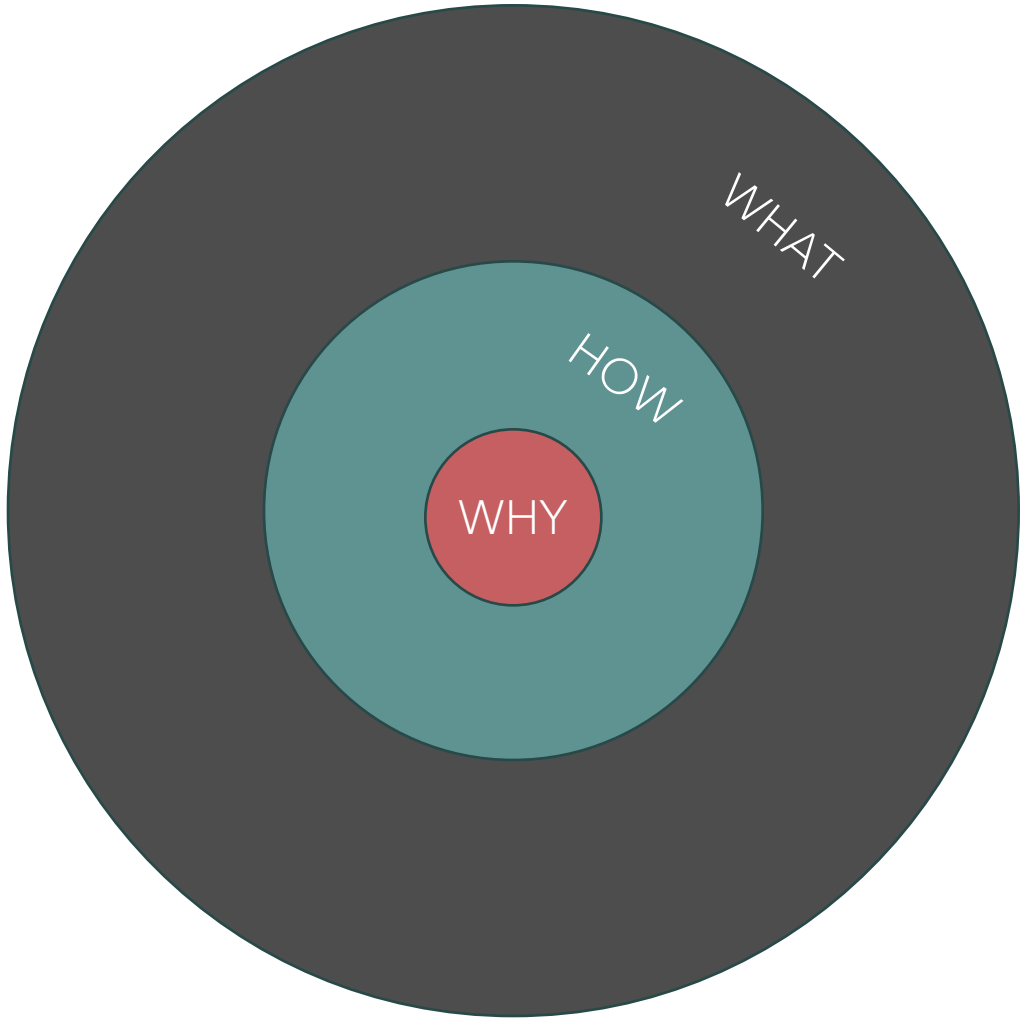
GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

alc Cyber Security Foundation+Practitioner CERTIFIED


START
HOW GREAT LEADERS INSPIRE
EVERYONE TO TAKE ACTION
WITH
SIMON SINEK
New York Times bestselling author of Leaders Eat Last and Together Is Better
WHY
MORE THAN
ONE MILLION
COPIES SOLD

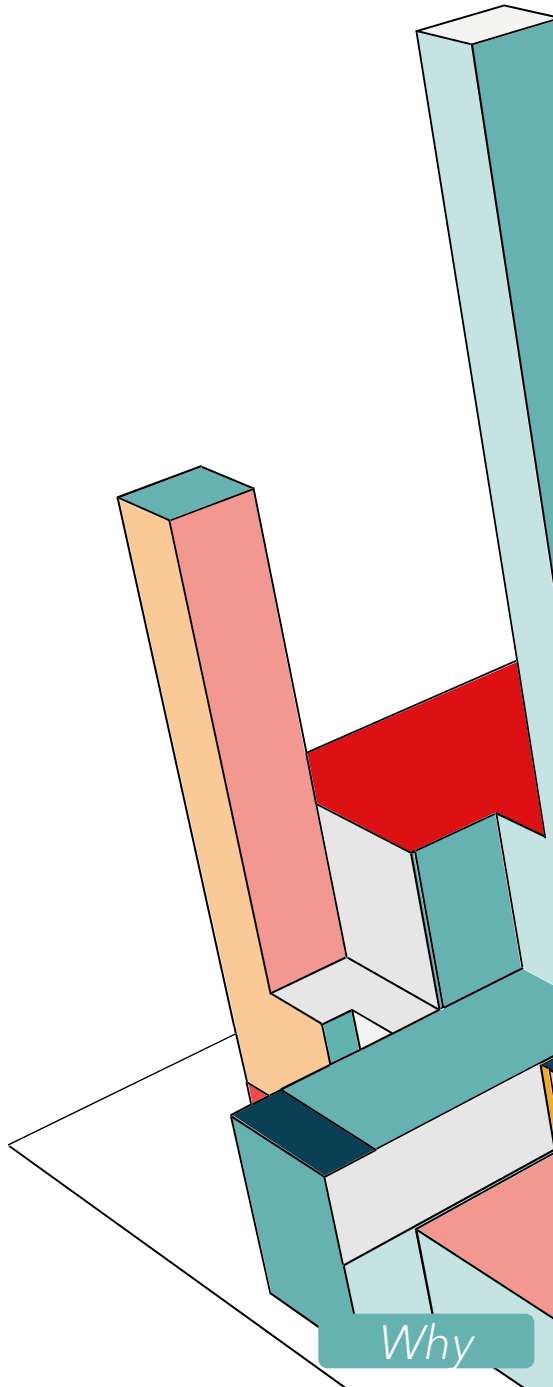
AGENDA

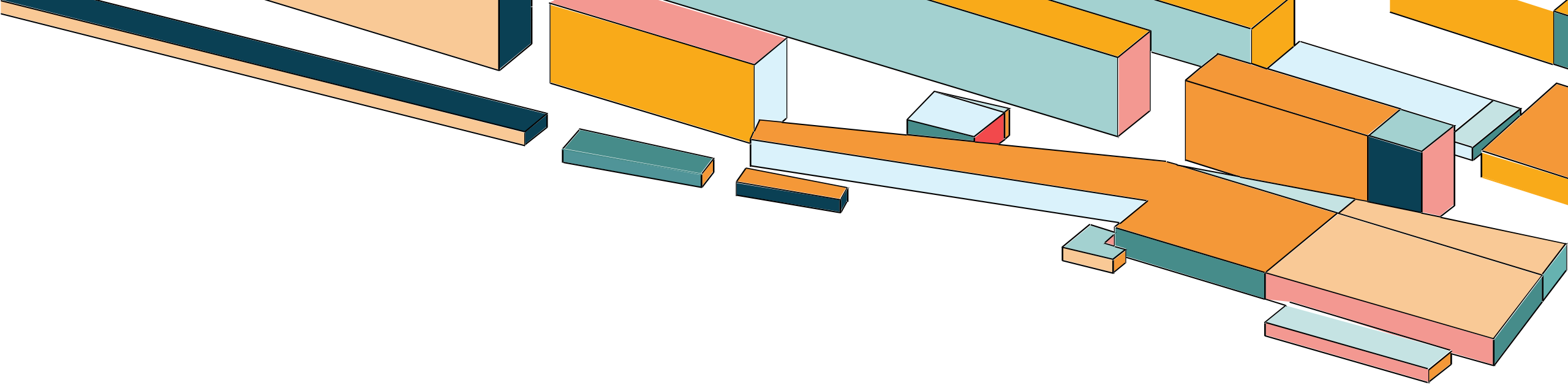


WHY ARCHITECTURE?

THE WHY COLUMN OF SABSA

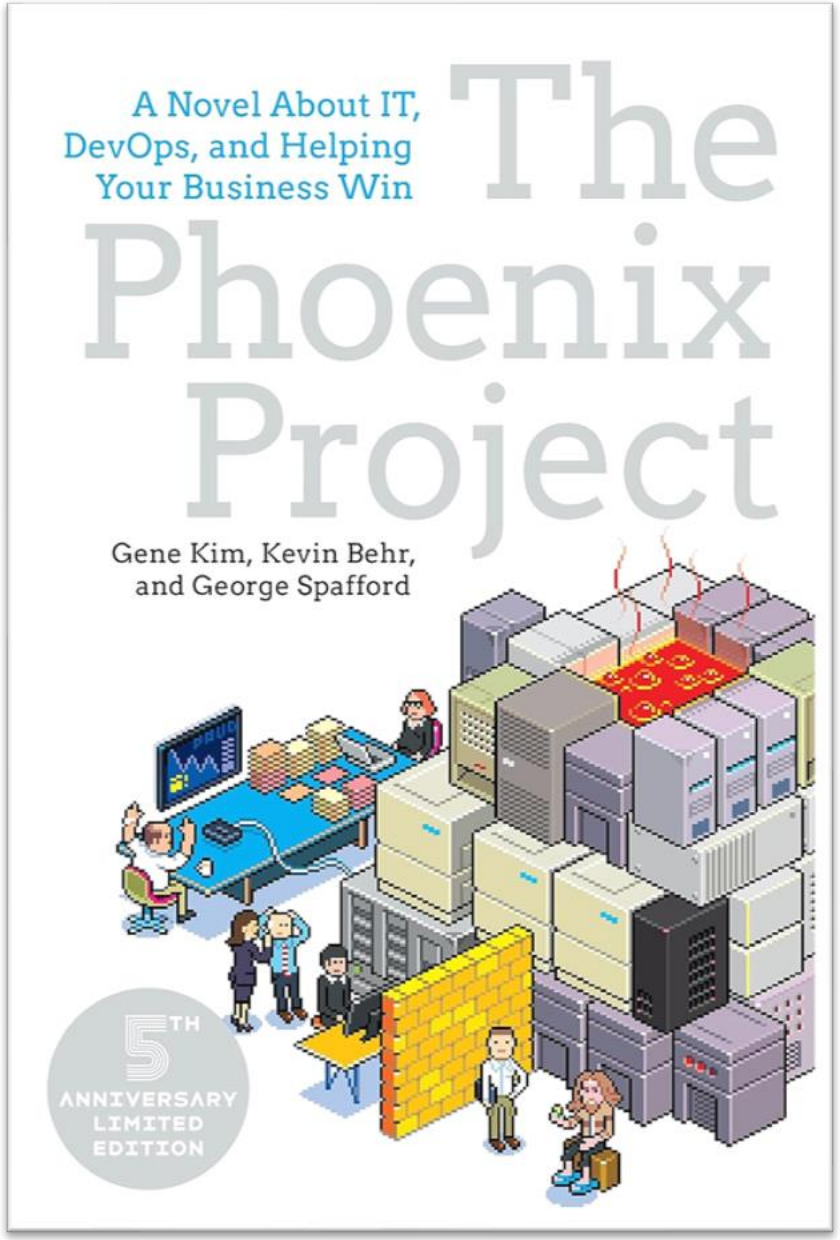
	MOTIVATION (Why)
CONTEXTUAL ARCHITECURE	Business Risk
	Opportunities & Threats Inventory
CONCEPTUAL ARCHITECTURE	Risk Management Objectives
	Enablement & Control Objectives; Policy Architecture
LOGICAL ARCHITECTURE	Risk Management Policies
	Domain Policies
PHYSICAL ARCHITECTURE	Risk Management Practices
	Risk Management Rules & Procedures
COMPONENT ARCHITECTURE	Risk Management Tools & Standards
	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools
SERVICE MANAGEMENT ARCHITECTURE	Operational Risk Management
	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment





HOW?

THE TIMING *DILEMMA* ...


A Novel About IT, DevOps, and Helping Your Business Win
The Phoenix Project
Gene Kim, Kevin Behr, and George Spafford
5TH ANNIVERSARY LIMITED EDITION

How

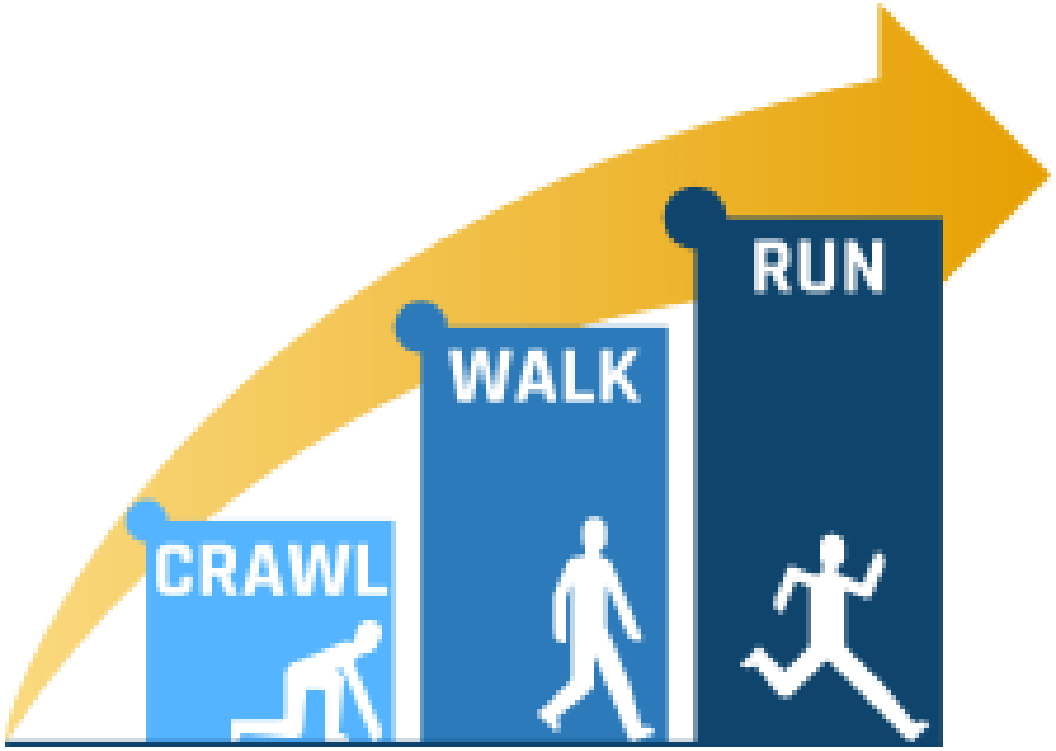
Waterfall

- Great for projects that we have done before and know what we are doing
- Essential for projects where it is difficult to *undo* prior work
- Can give the illusion of control e.g. Gantt Charts
- Started in IT when computing was *expensive*

Agile

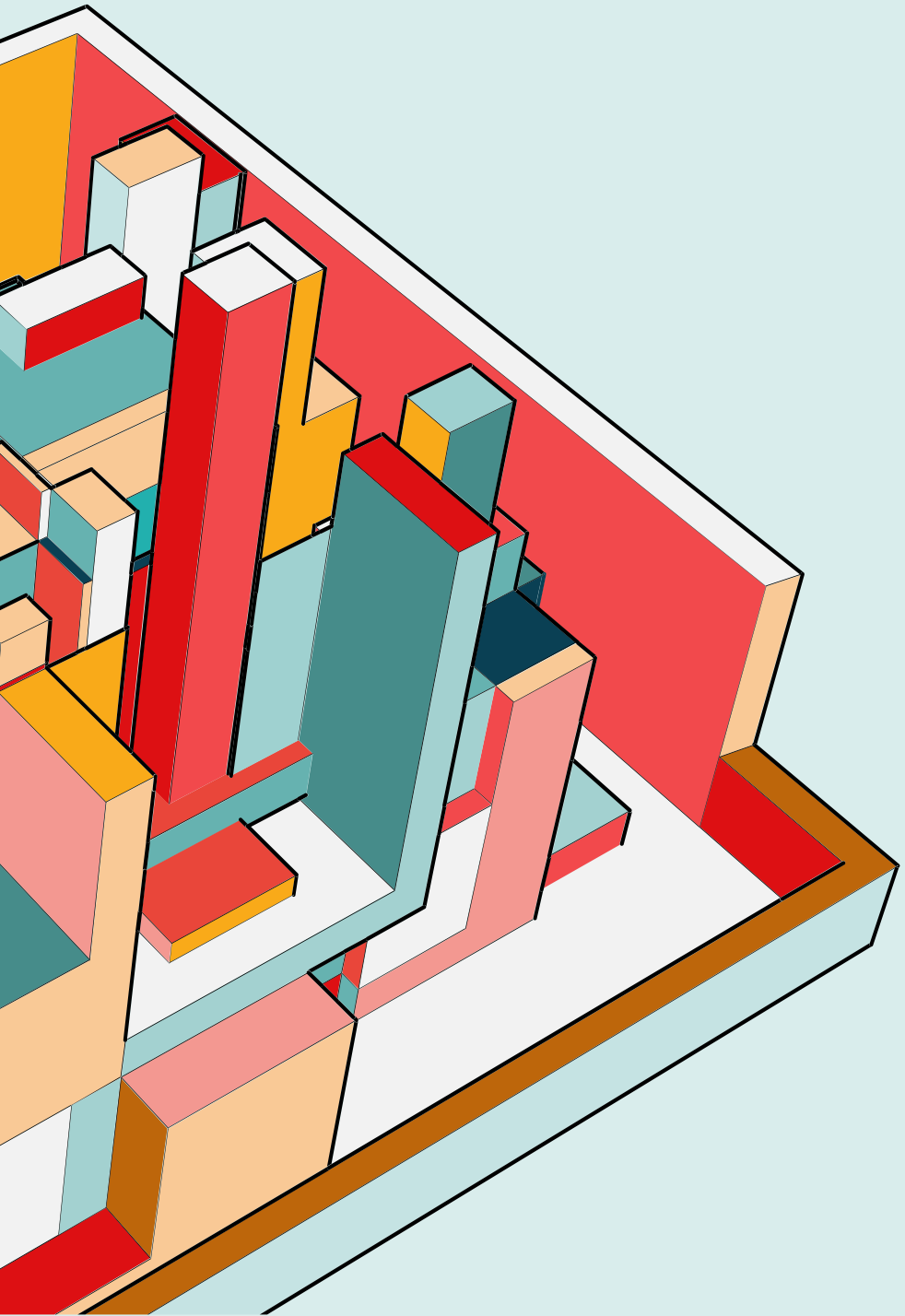
- The right approach for when we don't really know what we want
- Also, the right approach for when we don't really know what good looks like
- Prefers incremental delivery over "hail mary" big bang delivery
- Allows for experimentation and prioritises value delivery

CRAWL, WALK, RUN



Source - https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

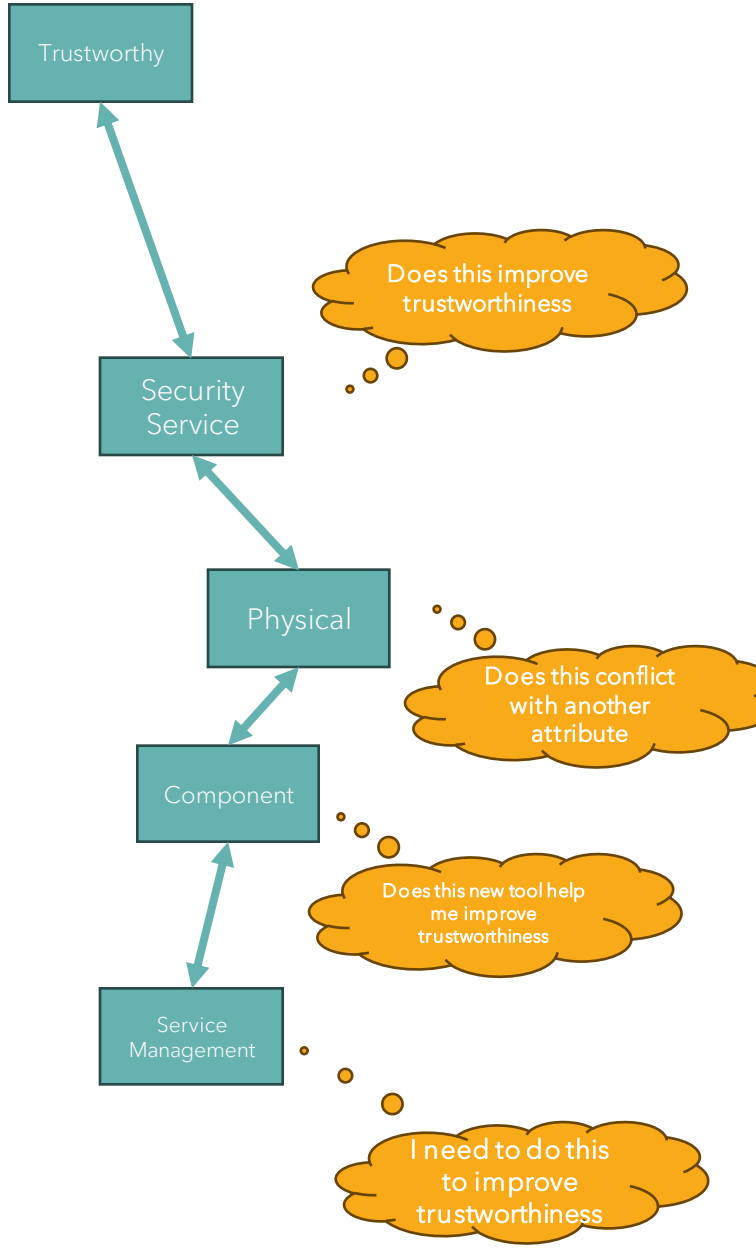
How



THE WHAT

FOR EXAMPLE … ATTRIBUTES

- Attributes are a foreign concept to most stakeholders
- They are however a **very smart abstraction** of cyber security requirements management
    - It provides a simple label for a complex interaction of security requirements to achieve a business goal
    - It can be used to highlight the impact of an emerging business driver on the enterprise's ability to exploit an opportunity or manage a risk
    - It uses the language of the stakeholder to make it relevant to the audience
    - It can cascade, interact and even disrupt other requirements
- But it is esoteric … so maybe don't start with them!



DELIVER A RIGHT SIZED APPROACH

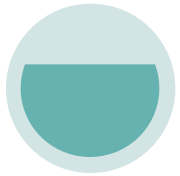
Crawl

Use Simple Frameworks like E8 or CIS CSC to guide Security Programs

Start with Vendor "best practice"

- System Hardening
- Cloud Hardening

Define Security Policies (maybe even *Generic ones …)*



Walk

Define Security Principles

Manage Security Requirements

Establish Security Zones

Use IT Service Management to support Cyber Security

Run

Enterprise Security Architecture as per SABSA

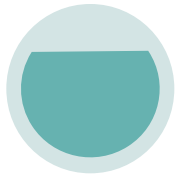
Partner with the business to manage risk whilst delivering value

Attributes Taxonomy

- Traceability for Justification and Completeness

Domain Modelling

Through Life Cyber Security Service Management



Jog?

SABSA FAST TRACK™

- Methodology to limit the scope to quickly deliver value via a Proof of Concept ESA
- Relies on intensive time-boxed expert facilitated workshops
- Should make use of software tools and automation
- There is some information regarding the approach outlined in the F1 & F2 materials and the Blue Book
- The Ask – Should we establish a Fast Track Working Group in TSI to produce an approach paper?

Ref – Blue Book *What*

MAPPING OF SABSA CONCEPTS TO WALK AND RUN

- Security Requirements <-> Attributes
- Network Zoning Model <-> Domain Model
- IT Service Management <-> Security Service Management
- Others? Your experience?

THE C2M2

- US DoE Cyber Security Capability Maturity Model
- Defines 10 domains
  - (ASSET) - Asset, Change, and Configuration Management
  - (THREAT) - - Threat and Vulnerability Management
  - (RISK) - Risk Management
  - (ACCESS) - Identity and Access Management
  - (SITUATION) - Situational Awareness
  - (RESPONSE) - Event and Incident Response, Continuity of Operations
  - (THIRD-PARTIES) - Third-Party Risk Management
  - (WORKFORCE) - Workforce Management
  - (ARCHITECTURE) - Cybersecurity Architecture
  - (PROGRAM) - Cybersecurity Program Management
- Has the Concept of Maturity Indicator Levels

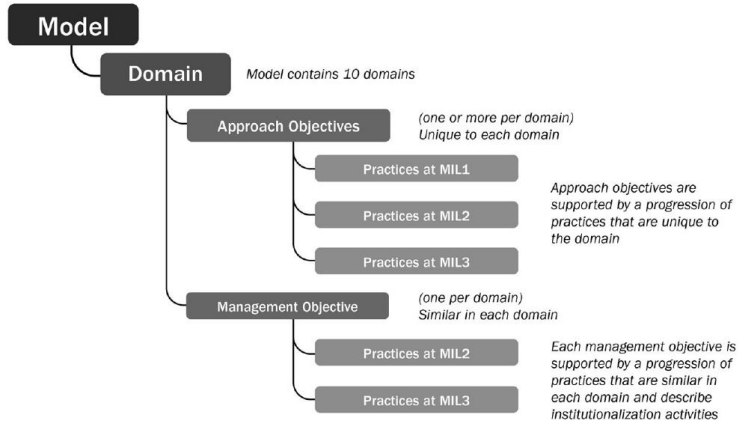


Figure 3: Model and Domain Elements

Table 4: Summary of Maturity Indicator Level Characteristics

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process Approach characteristic: • Practices are more complete or advanced than at MIL1
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives) • Responsibility, accountability, and authority for performing the practices are assigned • Personnel performing the practices have adequate skills and knowledge • The effectiveness of activities is evaluated and tracked Approach characteristic: • Practices are more complete or advanced than at MIL2

Source – C2M2 v2.1

What

THE C2M2 (CONT.)

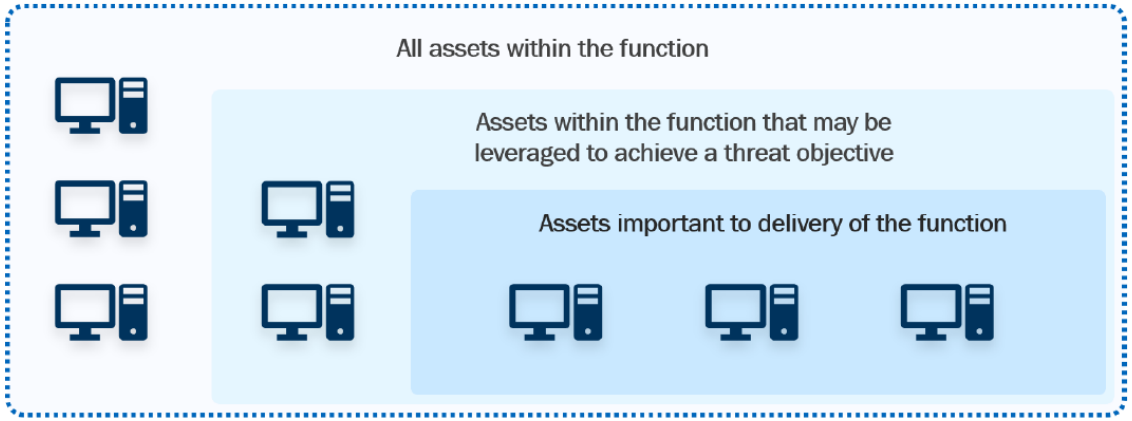


Figure 2: Groups of Assets

threat objective	Threat objectives are the potential outcomes of threat actor activities that are of concern because they would have negative impacts on the organization. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage. Threat actors may leverage multiple tactics or techniques, like those defined in the MITRE ATT&CK frameworks (for Enterprise or Industrial Control Systems) to achieve their goals. Threat objective examples include data manipulation, intellectual property theft, damage to property, denial of control, loss of safety, and operational outage.	C2M2

Source – C2M2 v2.1

What

REFERENCE – ARCHITECTURE ACCORDING TO THE C2M2

1. Establish and Maintain Cybersecurity Architecture Strategy and Program

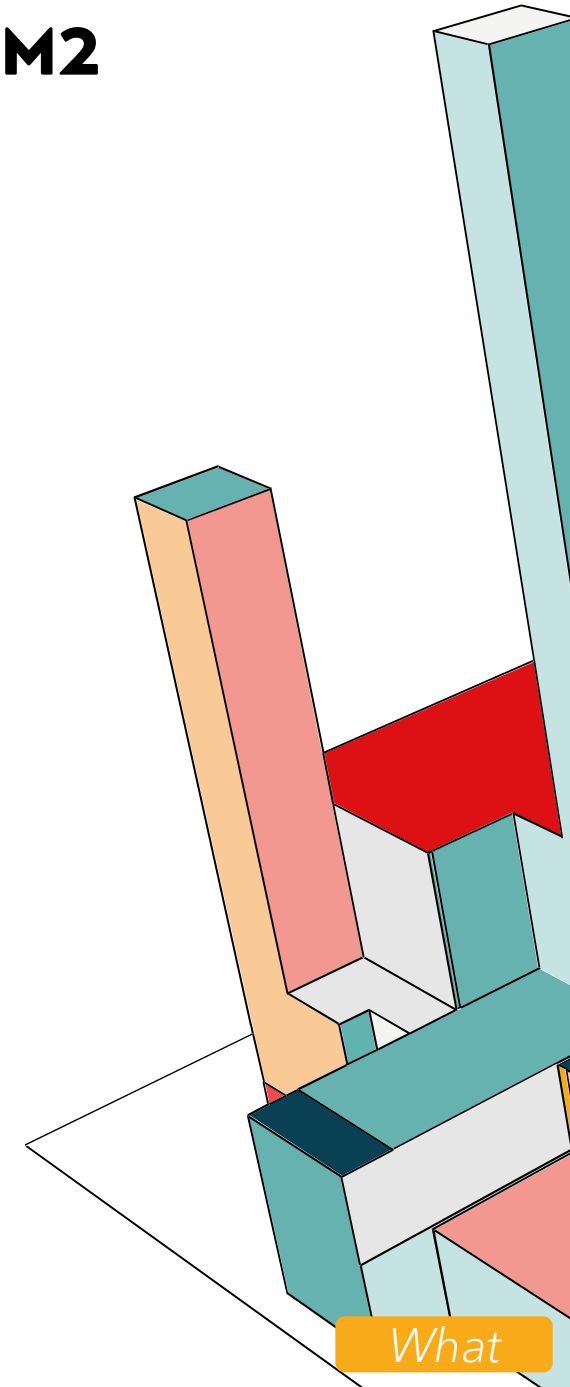
2. Implement Network Protections as an Element of the Cybersecurity Architecture

3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

4. Implement Software Security as an Element of the Cybersecurity Architecture

5. Implement Data Security as an Element of the Cybersecurity Architecture

6. Management Activities for the ARCHITECTURE domain



ESTABLISH AND MAINTAIN ARCH STRATEGY AND PROGRAM

MIL1

a. The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner

MIL2

b. A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise Architecture

c. A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization

d. Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process

e. Senior management sponsorship for the cybersecurity architecture program is visible and active

f. The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets

g. **Cybersecurity controls are selected and implemented to meet cybersecurity requirements**

MIL3

h. The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program

i. Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events

j. The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e)

k. The cybersecurity architecture addresses predefined states of operation (SITUATION-3g)

Source – C2M2 v2.1 *What*

IMPLEMENT NETWORK PROTECTIONS AS AN ELEMENT OF THE CYBERSECURITY ARCHITECTURE

MIL1

a. Network protections are implemented, at least in an ad hoc manner

b. The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner

MIL2

c. Network protections are defined and enforced for selected asset types according to asset risk and priority

d. Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements

e. Network protections incorporate the principles of least privilege and least functionality

f. Network protections include monitoring, analysis, and control of network traffic for selected security zones

g. Web traffic and email are monitored, analyzed, and controlled

MIL3

h. All assets are segmented into distinct security zones based on cybersecurity requirements

i. Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication

j. OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems

k. Device connections to the network are controlled to ensure that only authorized devices can connect

l. The cybersecurity architecture enables the isolation of compromised assets

Source – C2M2 v2.1

What

IMPLEMENT SOFTWARE SECURITY AS AN ELEMENT OF THE CYBERSECURITY ARCHITECTURE

MIL1

a. No practice at MIL1

MIL2

b. Software developed in-house for deployment on higher priority assets is developed using secure software development practices

c. The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices

d. Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house

MIL3

e. All software developed in-house is developed using secure software development practices

f. The selection of all procured software includes consideration of the vendor's secure software development practices

g. The architecture review process evaluates the security of new and revised applications prior to deployment

h. The authenticity of all software and firmware is validated prior to deployment

i. Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events

Source – C2M2 v2.1

What

IMPLEMENT DATA SECURITY AS AN ELEMENT OF THE CYBERSECURITY ARCHITECTURE

MIL1

a. Sensitive data is protected at rest, at least in an ad hoc manner

MIL2

b. All data at rest is protected for selected data categories
c. All data in transit is protected for selected data categories
d. Cryptographic controls are implemented for data at rest and data in transit for selected data categories
e. Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls
f. Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented

MIL3

g. The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen
h. The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data

Source – C2M2 v2.1

What

MANAGEMENT ACTIVITIES FOR THE ARCHITECTURE DOMAIN

MIL1	MIL2	MIL3
a. No practice at MIL1	b. Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain c. Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain	d. Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain e. Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel f. Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities g. The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked

Source – C2M2 v2.1 *What*

FOR EXAMPLE, WHAT DOES IT LOOK LIKE AT MIL-1

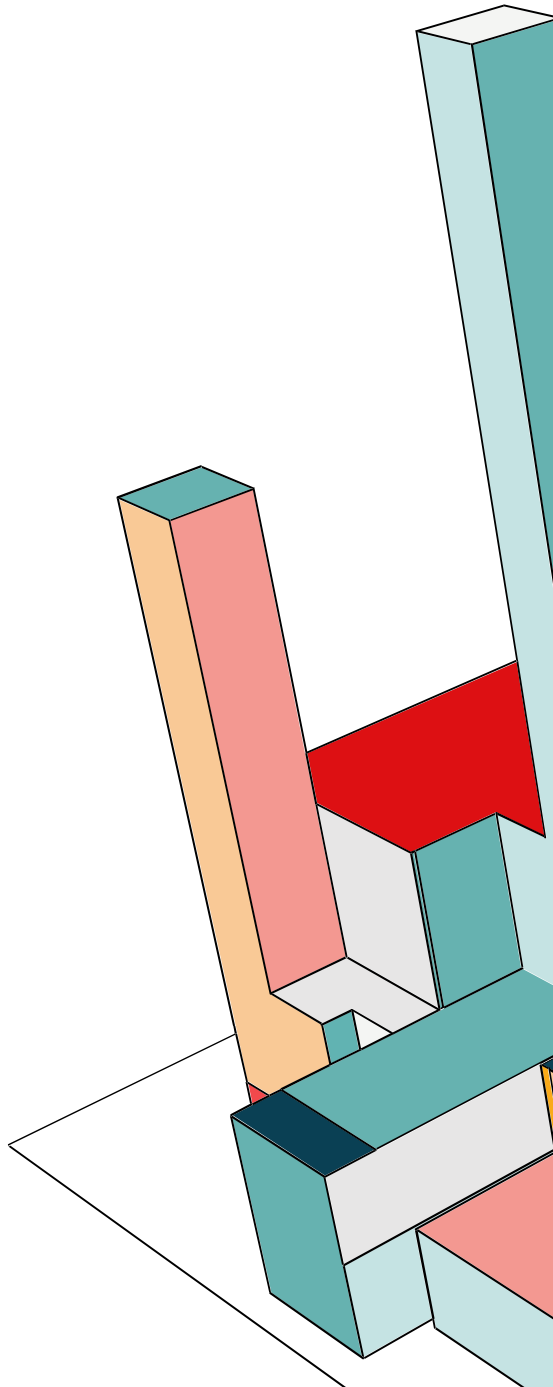
1. Establish and Maintain Cybersecurity Architecture Strategy and Program	• The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner
2. Implement Network Protections …	• Network protections are implemented, at least in an ad hoc manner • The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner
3. Implement IT and OT Asset Security …	• Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner • Endpoint protections are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner
4. Implement Software Security …	• No practice at MIL1
5. Implement Data Security …	• Sensitive data is protected at rest, at least in an ad hoc manner
6. Management Activities	• No practice at MIL1

Source – C2M2 v2.1

What

SUMMARY

- Remember to start with the why with your stakeholders (Start with the Why)
- Incremental delivery is always better than big bang (Phoenix Project)
- Crawl, Walk and Run – don't skip straight to run …
    - Try a Jog (SABSA Fast Track™)
    - Should we establish a SABSA Fast Track Working Group?
- Think about how you incrementally build ESA concepts on your journey
- The C2M2 is a useful reference and you can use the Maturity Indicator Levels (MIL) to plan your progression



THANK YOU, QUESTIONS?

https://linkedin.com/in/blargeau

https://github.com/beLarge

@beLarge