Architecture at Scale

Save time. Reduce spend. Increase security.

Ryan Elkins

@the_ryan_elkins

ryan-elkins@outlook.com

Agenda

- Build a security architecture program that will work effectively.
  - Why it is important.
  - Why it is a challenge.
  - What not to do.
  - What to do.
  - How to automate it.

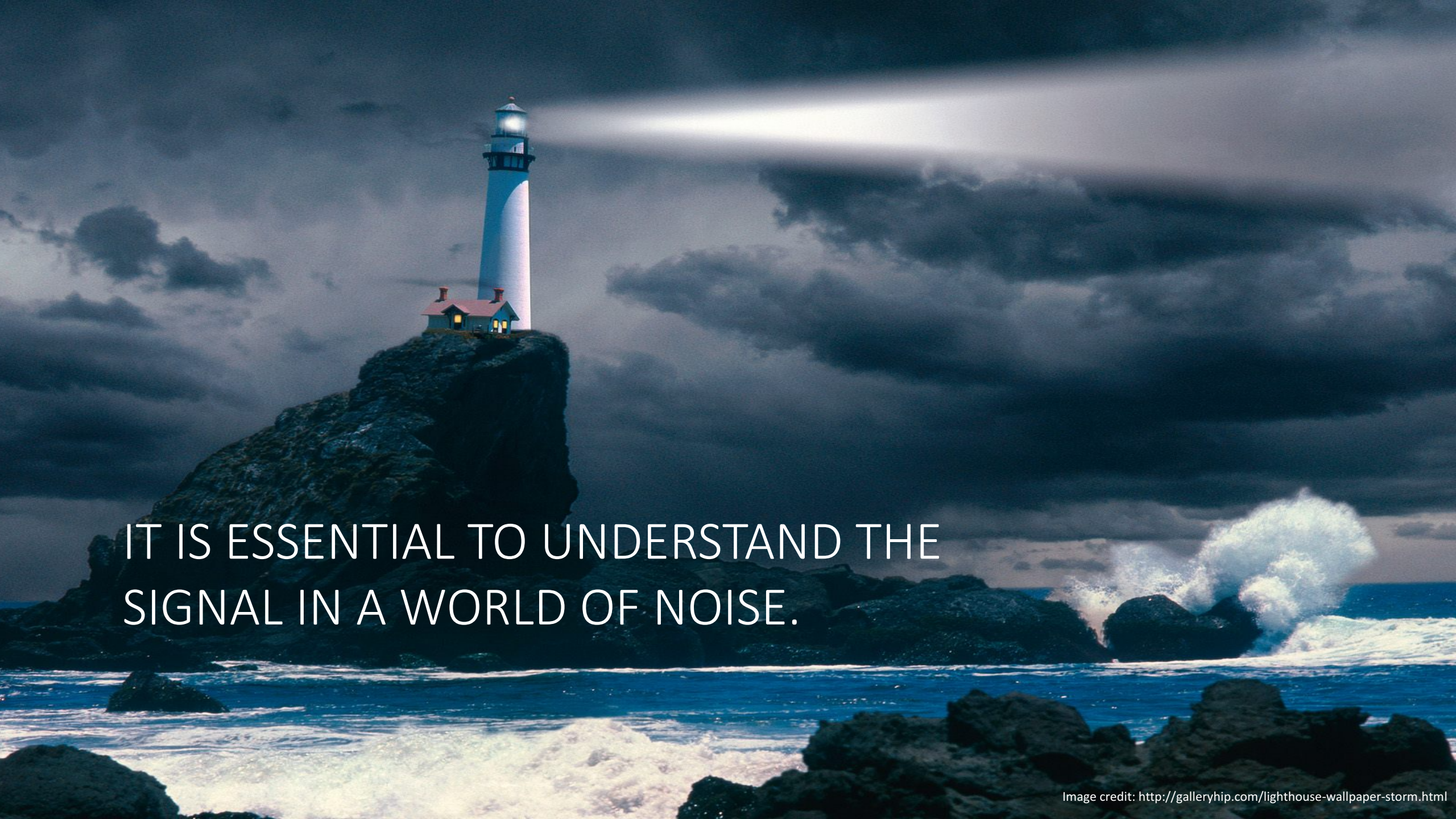
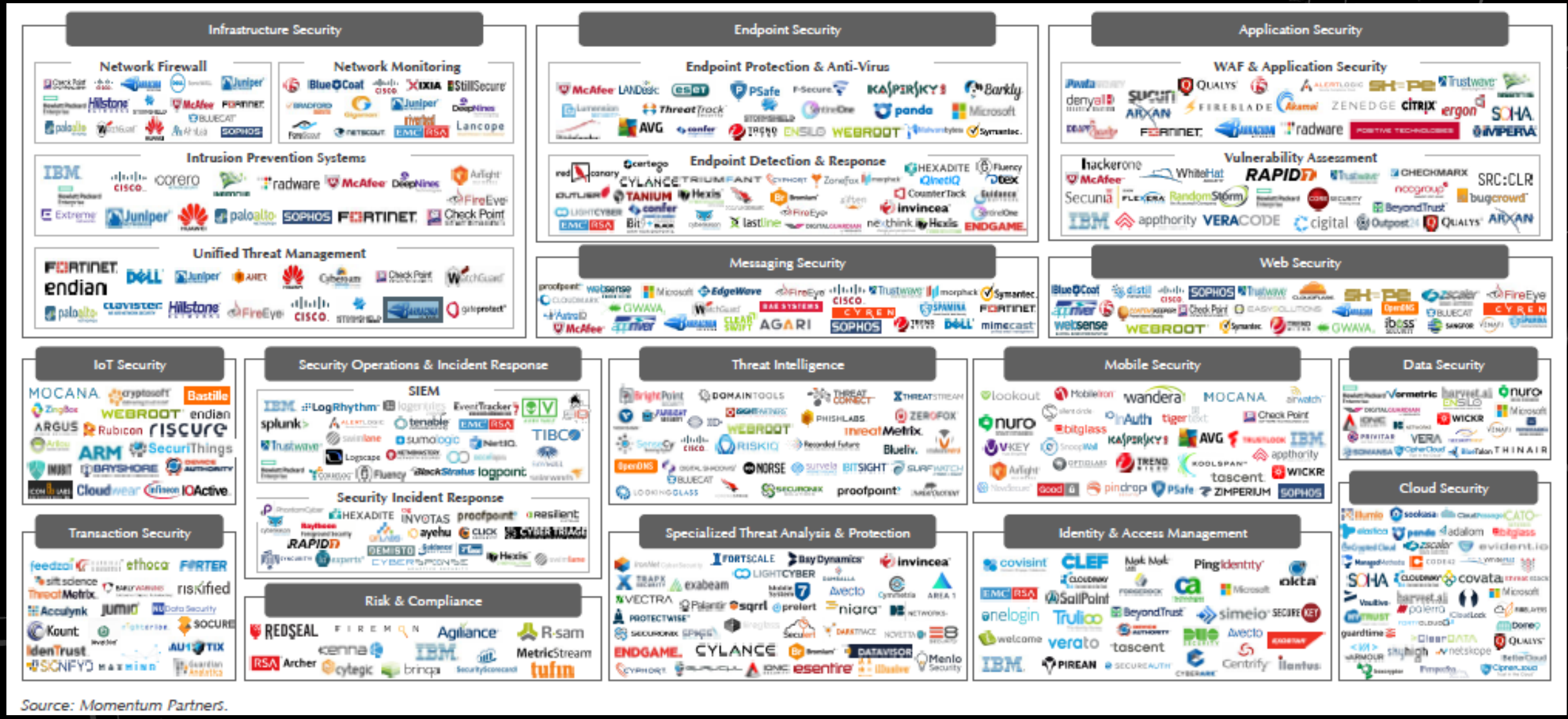


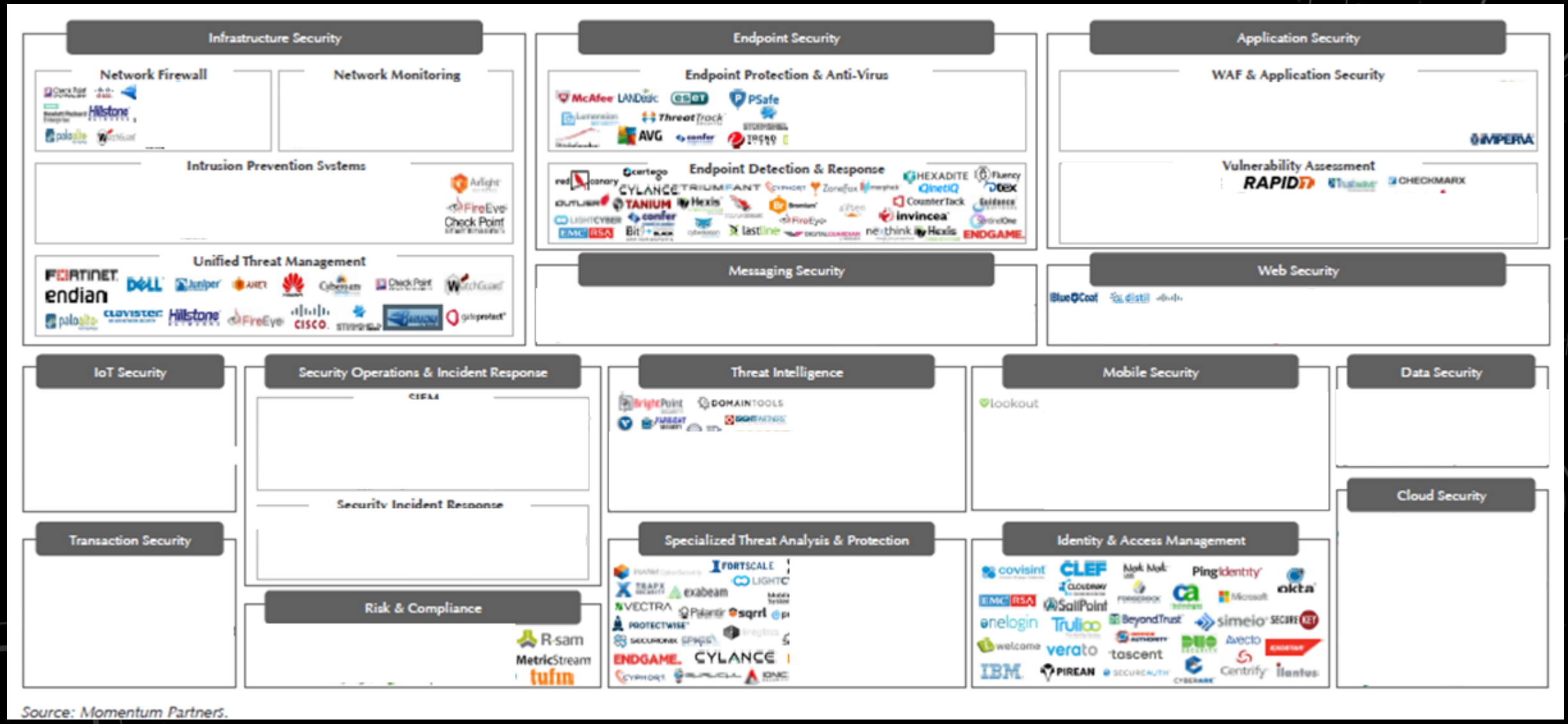
Image credit: http://galleryhip.com/lighthouse-wallpaper-storm.html

Vendors say that you need this.



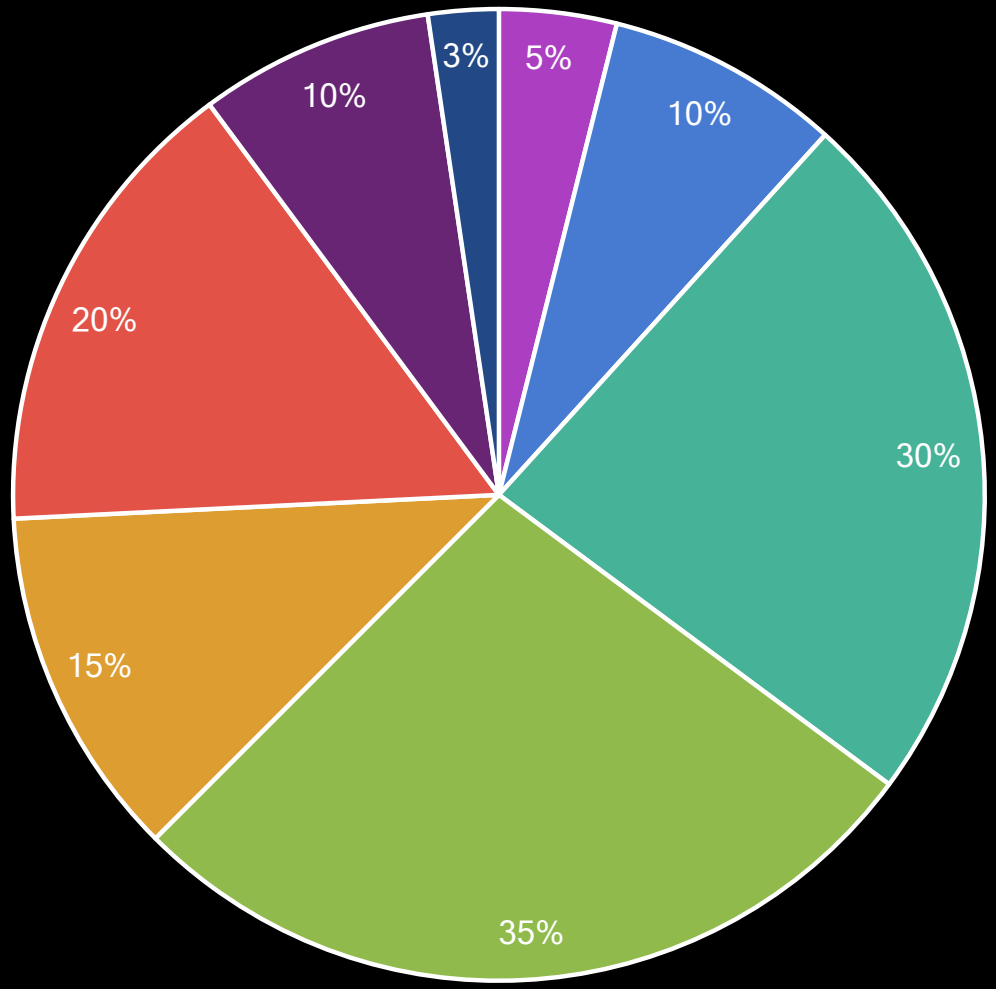
Source: Momentum Partners.

Without strategy, you want this.



Source: Momentum Partners.

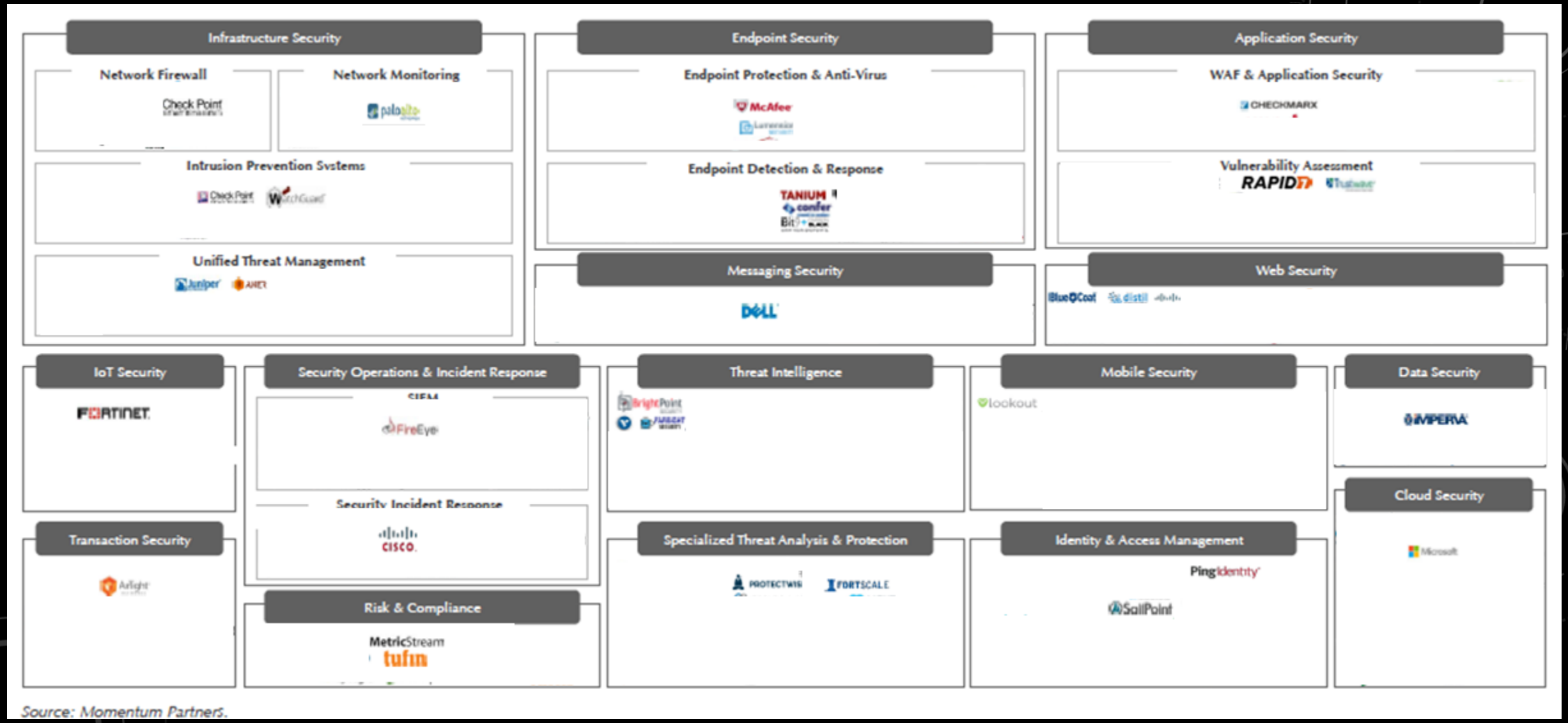
You evaluate current budgetary allocations.



You realize you can afford this.

Your boss expects this.

You actually need this.



Source: Momentum Partners.

YOU CANNOT BUY SECURITY

WHERE DO YOU BEGIN?

Everything must begin and end with risk.

Risk = Likelihood x Impact

Look at your business – understand the impact.

- What is most critical to the business?
  - Is it service driven where availability is critical?
  - Is it customer data driven where data records are critical?
  - Is it product driven where blueprints and trade secrets are critical?
- How can these most critical areas be impacted (threats)?

Look at the news – understand the threat.

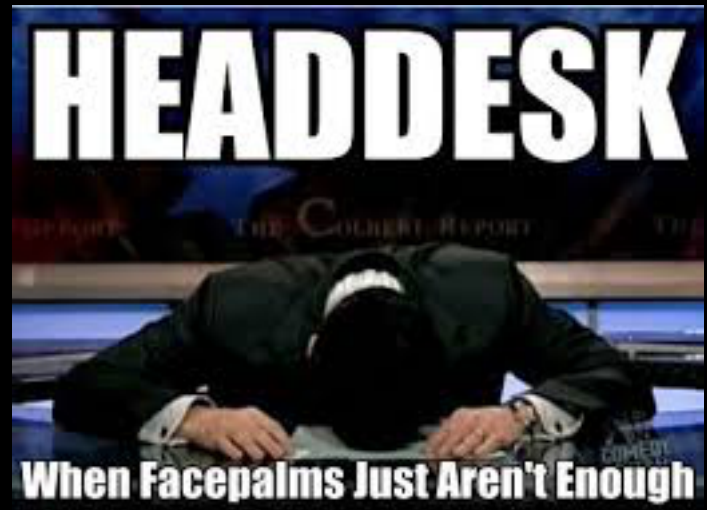
- Have other companies within the same industry been affected?
- How did the data breaches occur?
- What was stolen or compromised?
- Are the correct controls in-place to prevent the same thing from happening?
- Do nation states, competitors, hacktivists, or cyber criminals have a motive to target the company?

Look at your program – understand the exposure.

- Do the initiatives align and support the business?
- Is the program focused on the correct areas?
- Are there any major vulnerabilities or control gaps?
- Is there leadership support for the program?

OK, GREAT. NOW I REALIZE THAT:

Impact = Company would go out of business if a breach occurs.
Threat = Our intellectual property is worth billions. Everyone wants it.
Exposure = We think there are gaps, but not really sure.



WE DO HAVE OPTIONS:

WE DO HAVE OPTIONS:

1. WE THROW IN THE TOWEL.

WE DO HAVE OPTIONS:

1. WE THROW IN THE TOWEL.
2. WE BURNOUT AND CHANGE FIELDS.

WE DO HAVE OPTIONS:

1. WE THROW IN THE TOWEL.
2. WE BURNOUT AND CHANGE FIELDS.
3. WE GET A CONSULTING JOB TO TELL OTHERS HOW BAD THEIR SECURITY IS.

3 REASONS WHY PEOPLE, PROGRAMS, AND COMPANIES FAIL

*I did not join the security field to lose.

Failure to see.

Failure to act.

Failure to finish.

Why architecture fails.

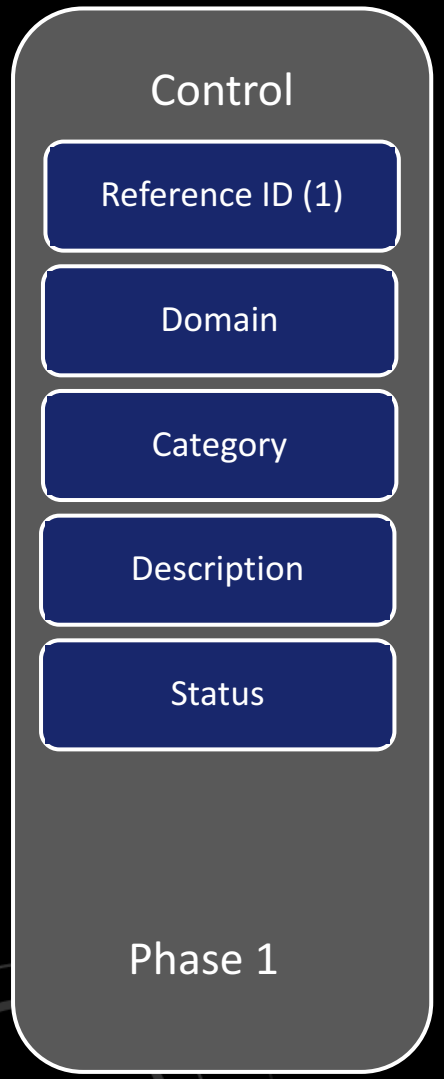
- The cart comes before the horse.
- Most programs begin operational and then introduce architecture.
- Isolation from the business, IT, and the rest of Information Security
- There is too much complexity at once:
  - SABSA, DoDAF, TOGAF, MODAF, OSA, Zachman, CEB

Architecture must be viewed as a transformational function.

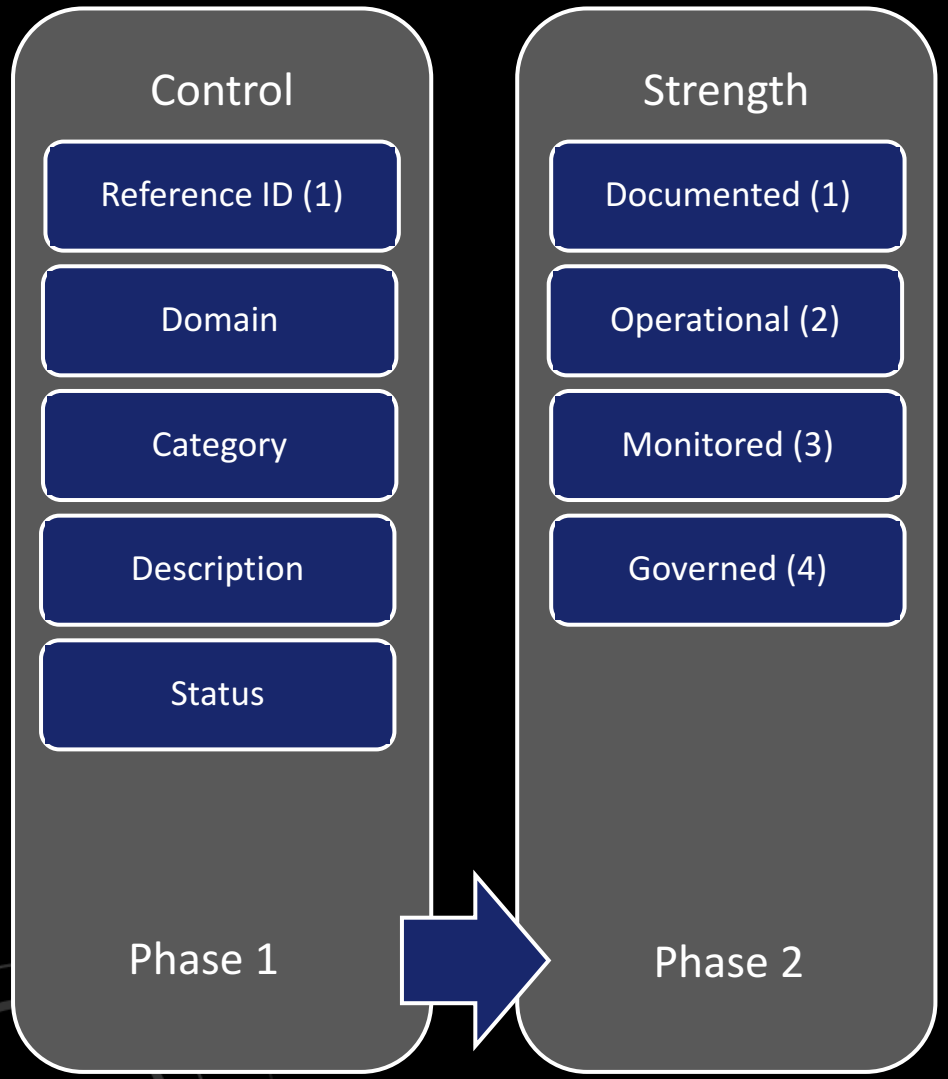
Establish the architecture

- The core architecture must:
  - Be agile to support change.
  - Visionary to support enterprise strategy.
  - Reasonable to support adoption.

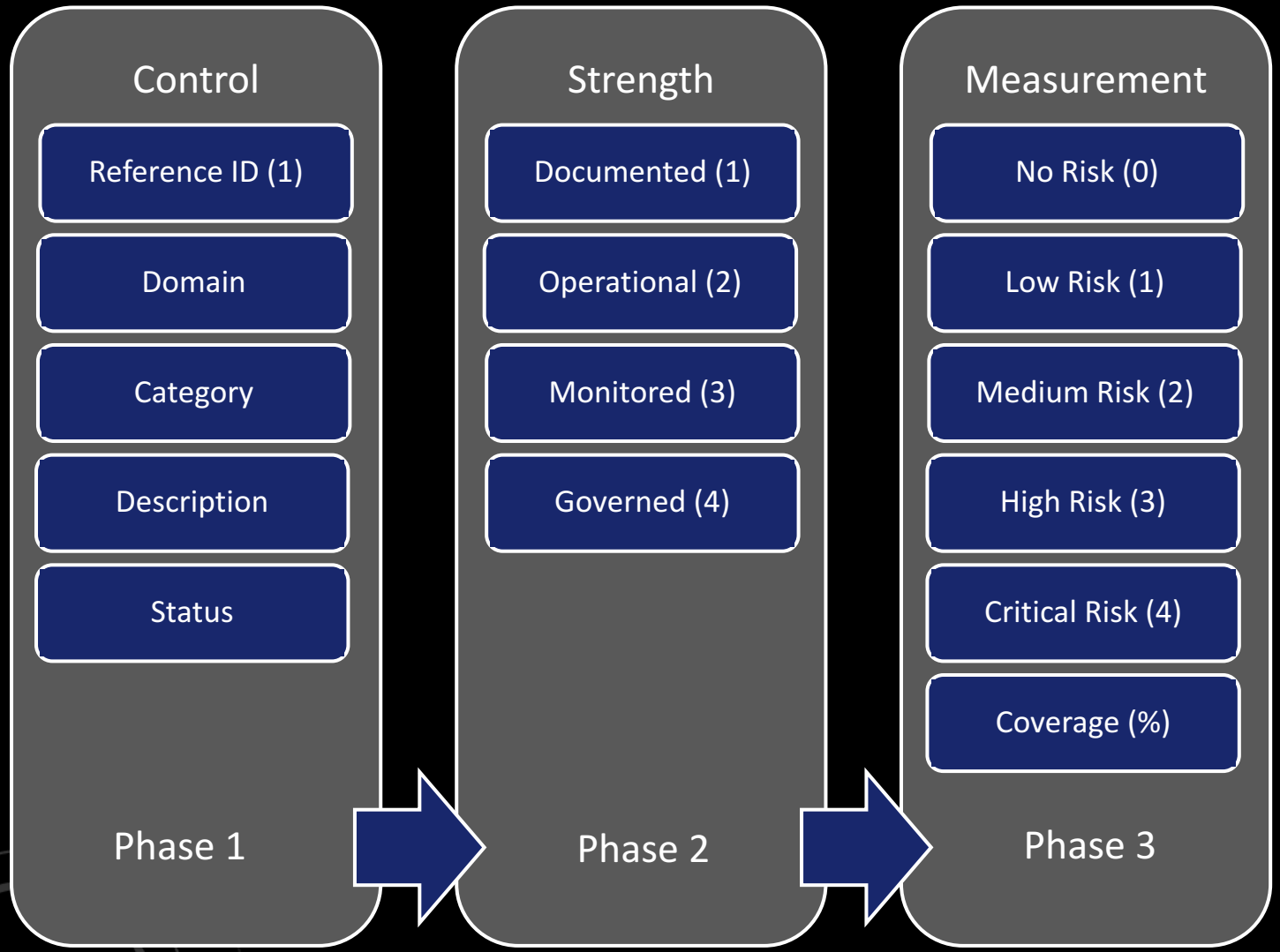
Control Framework - Phase 1



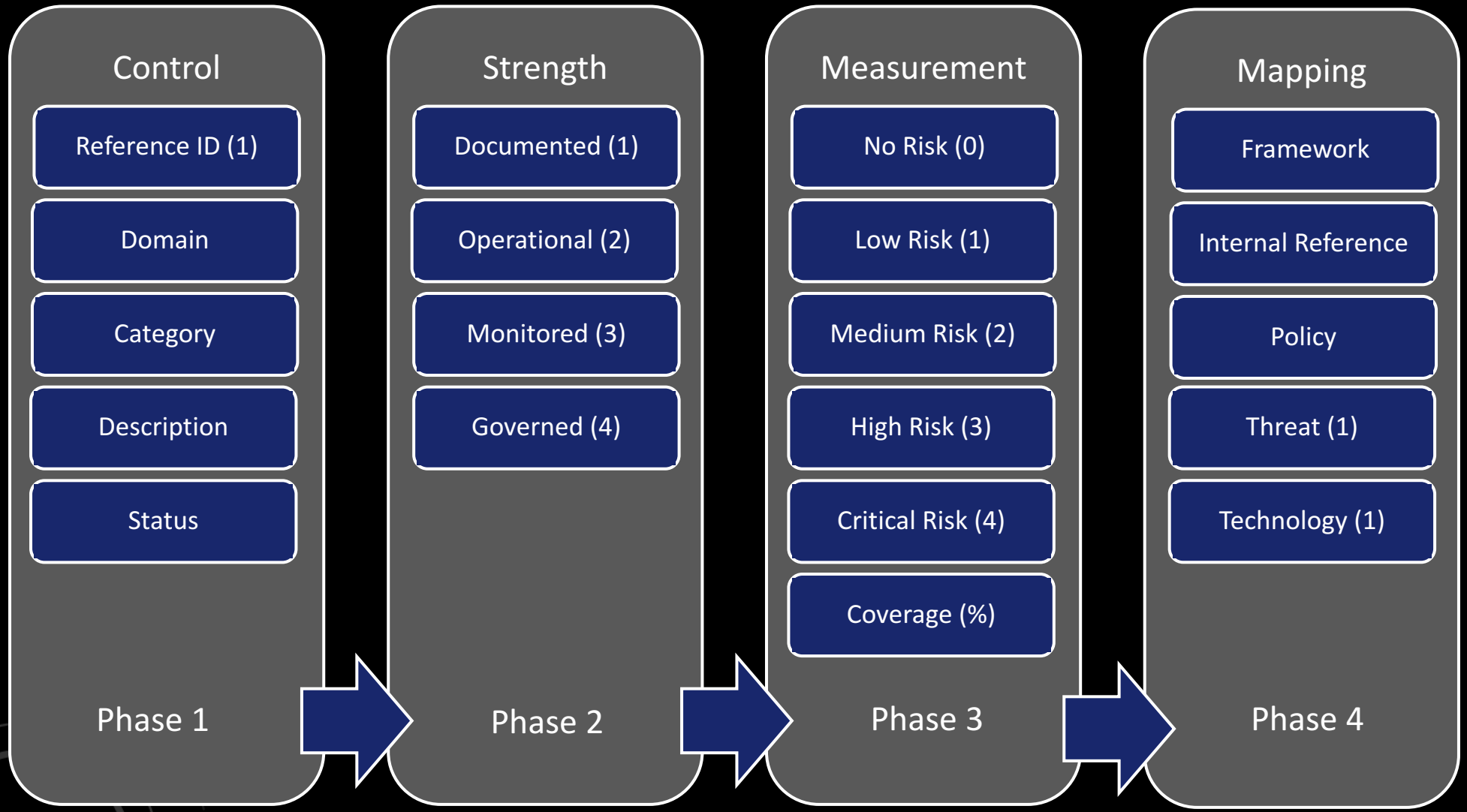
Control Framework – Phase 2



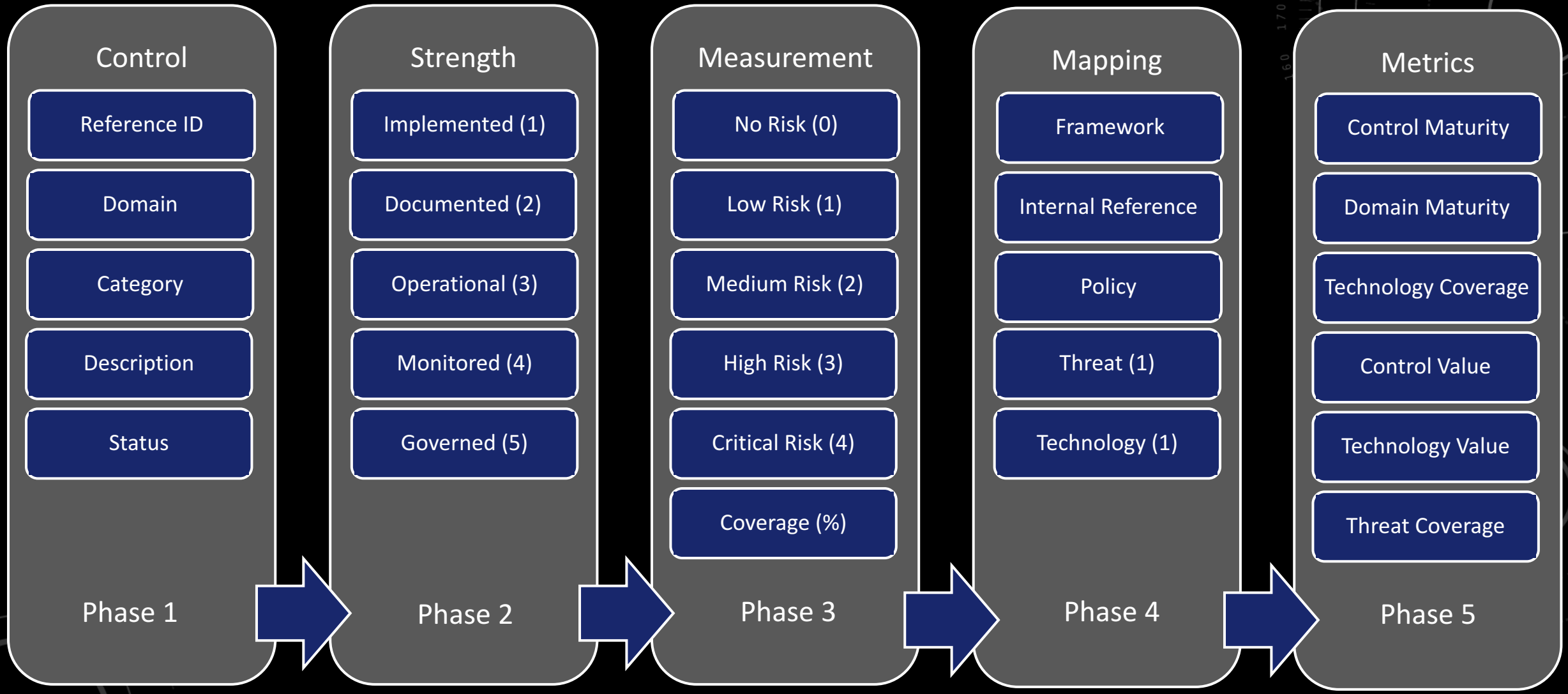
Control Framework – Phase 3



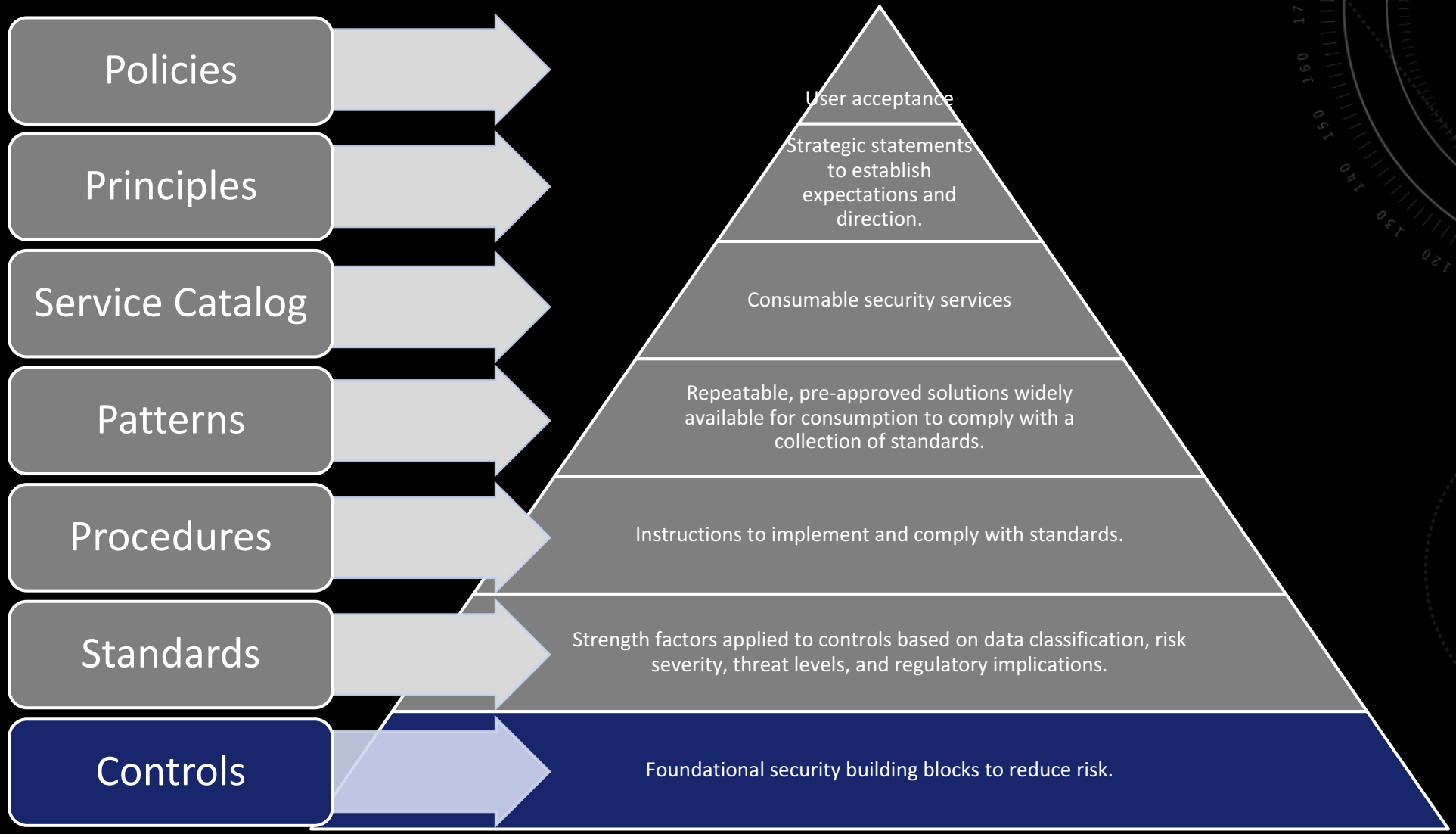
Control Framework – Phase 4



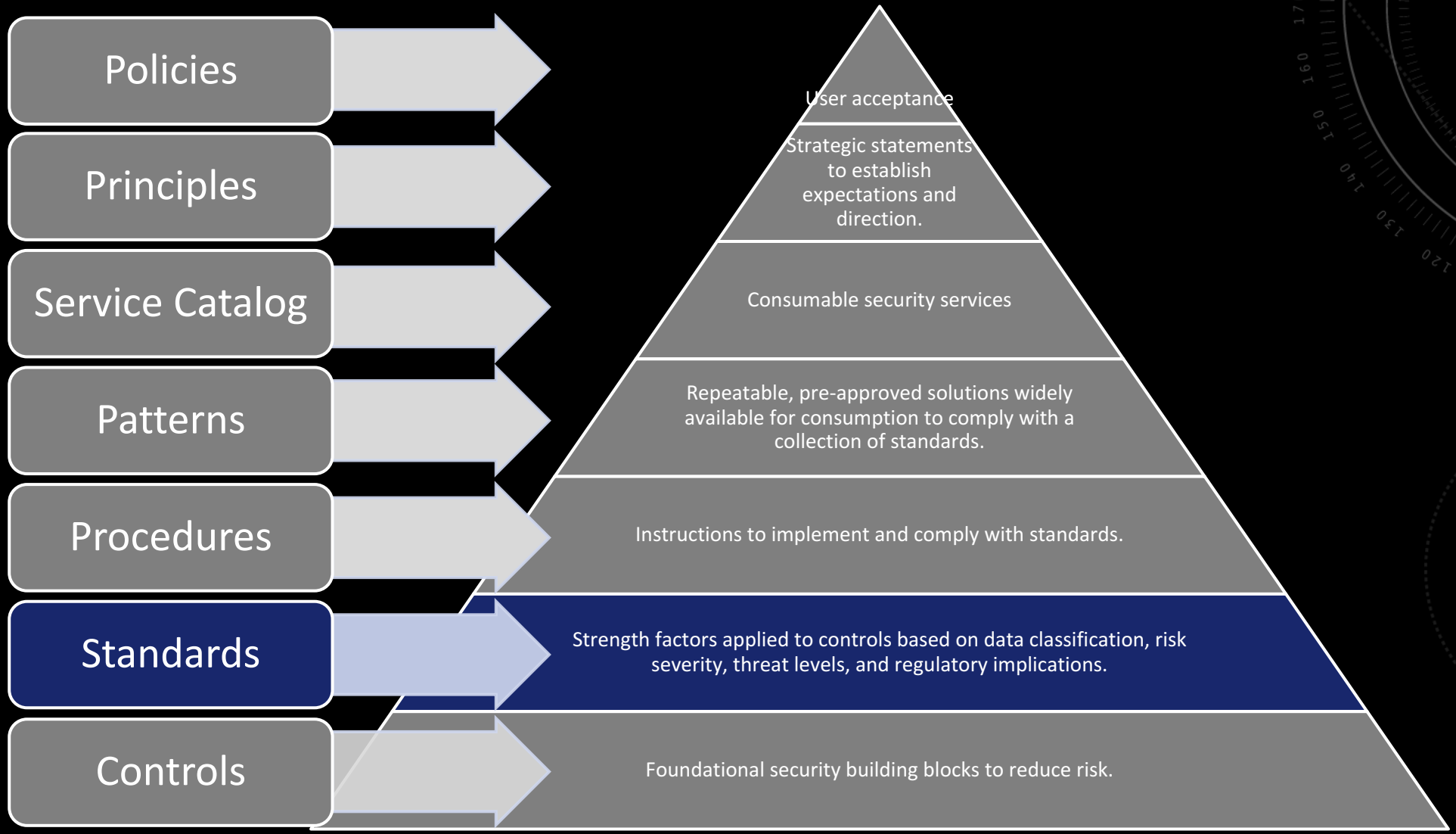
Control Framework – Phase 5



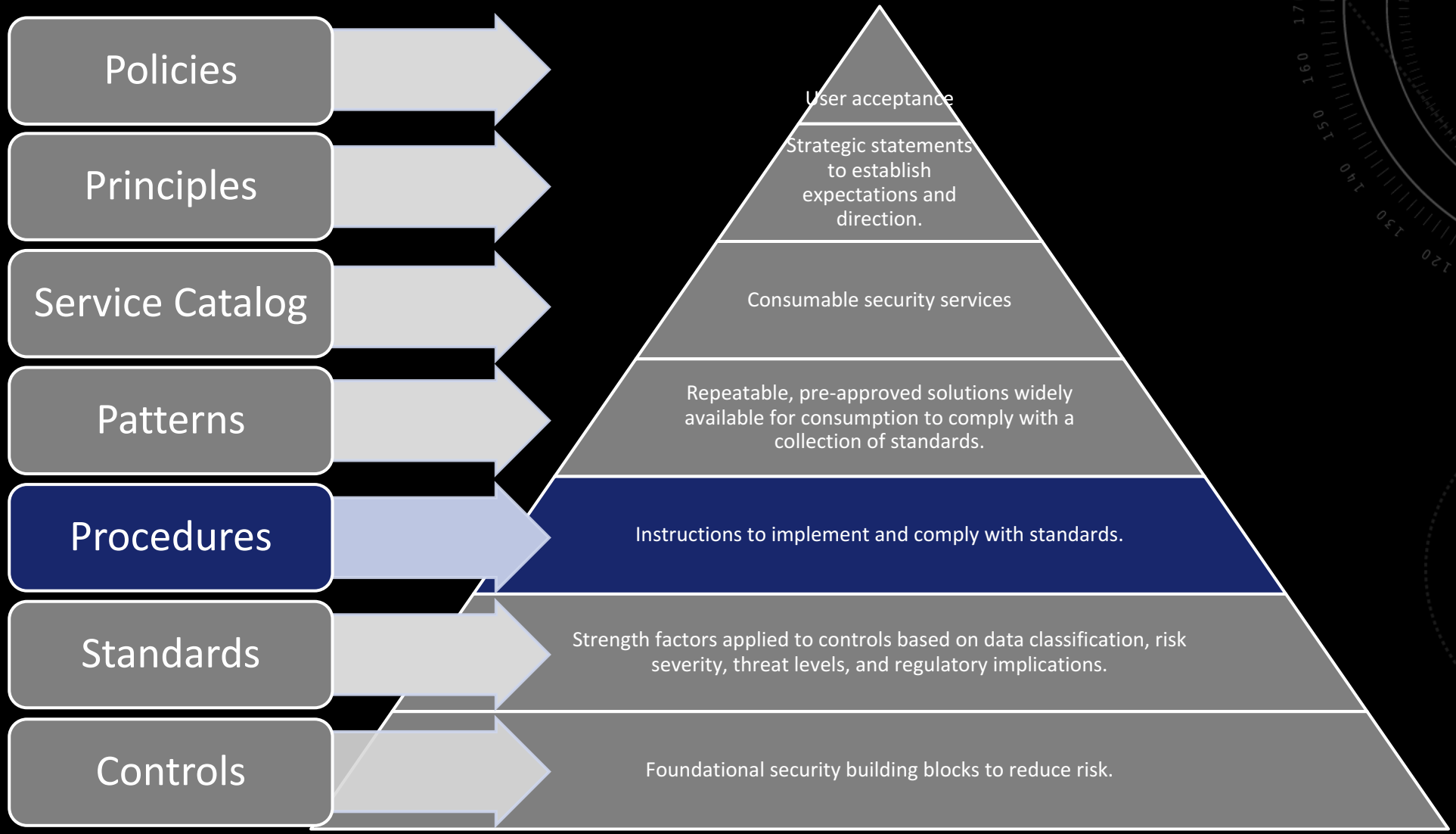
Architecture-at-scale



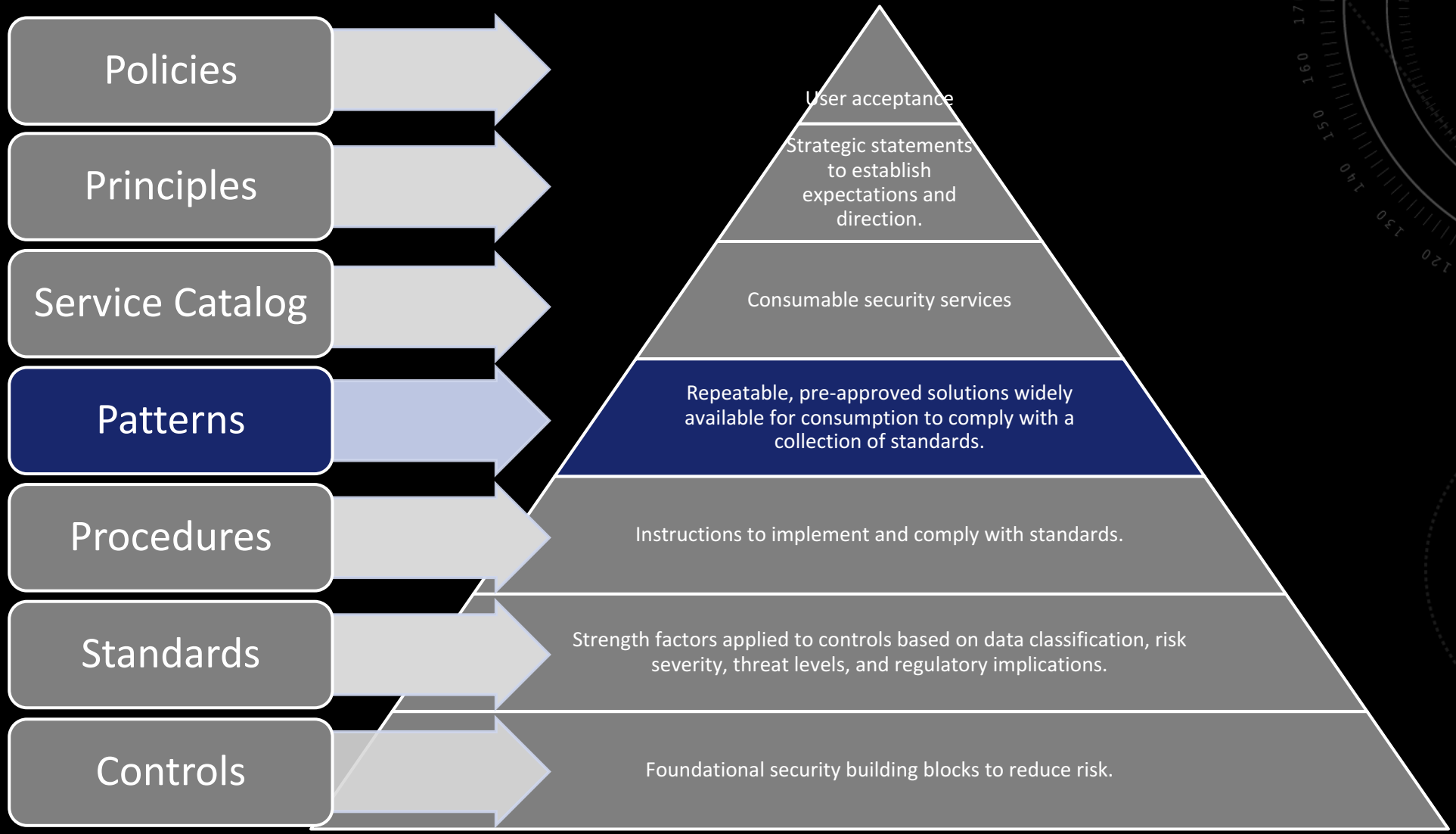
Architecture-at-scale



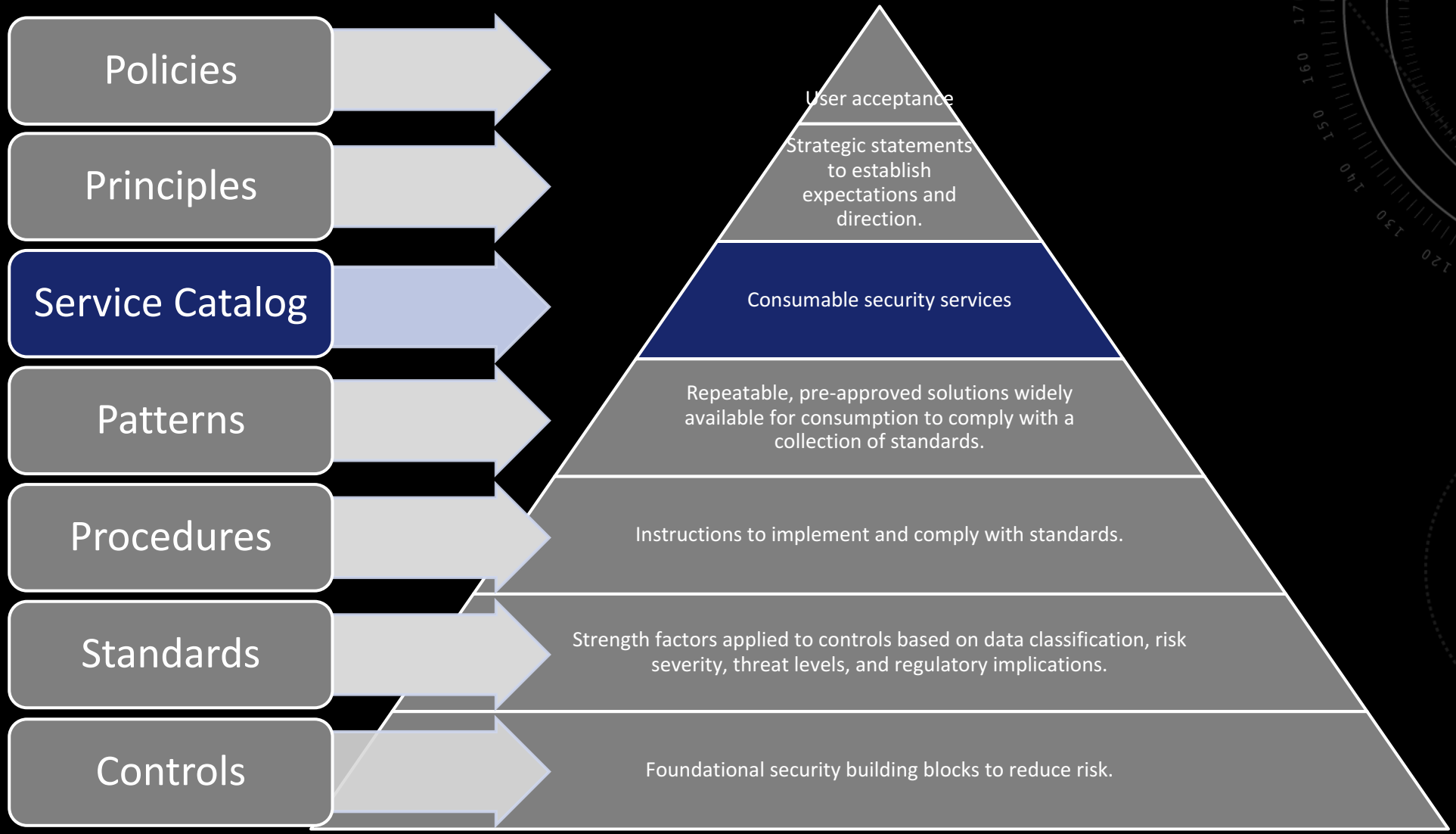
Architecture-at-scale



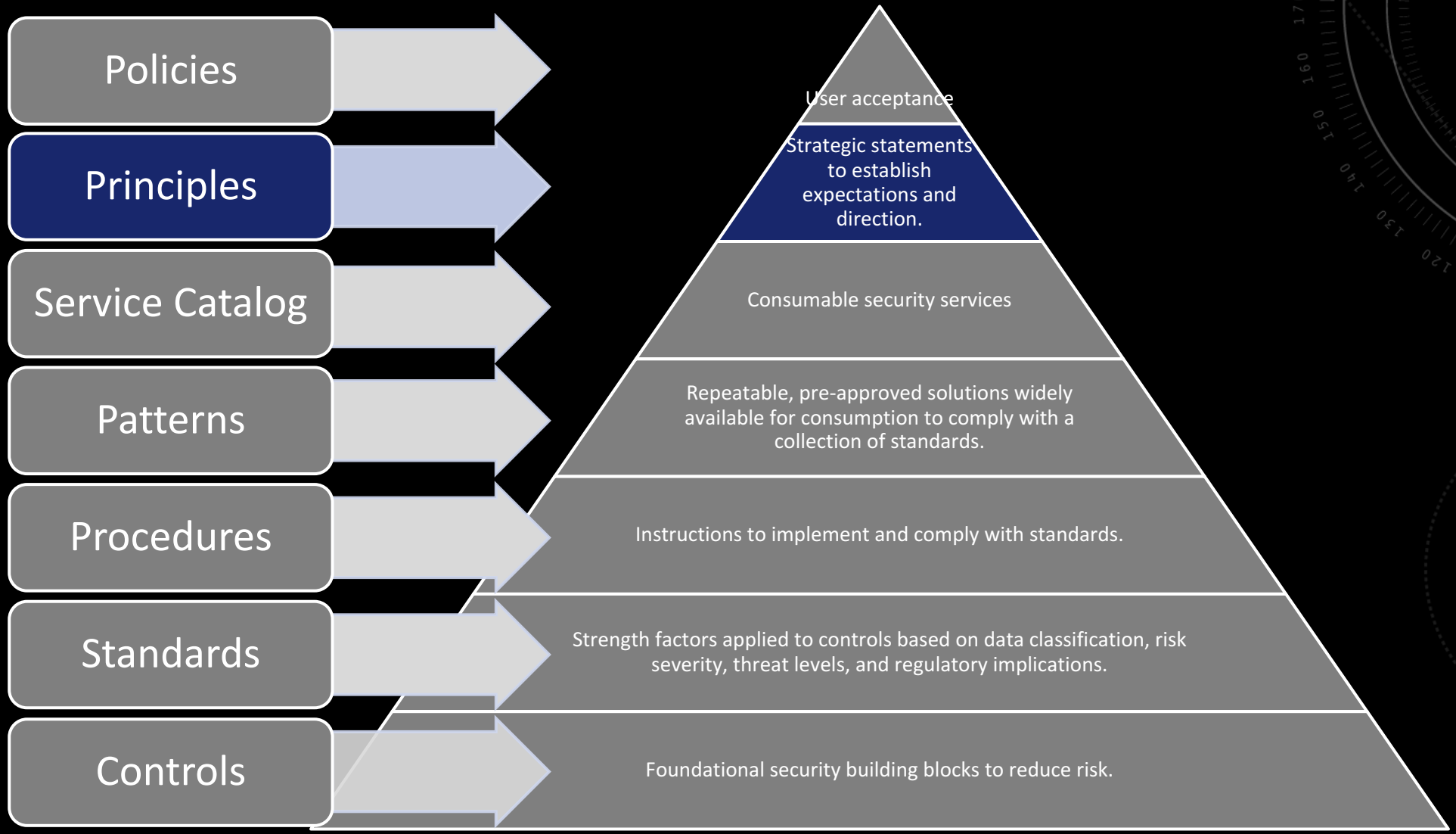
Architecture-at-scale



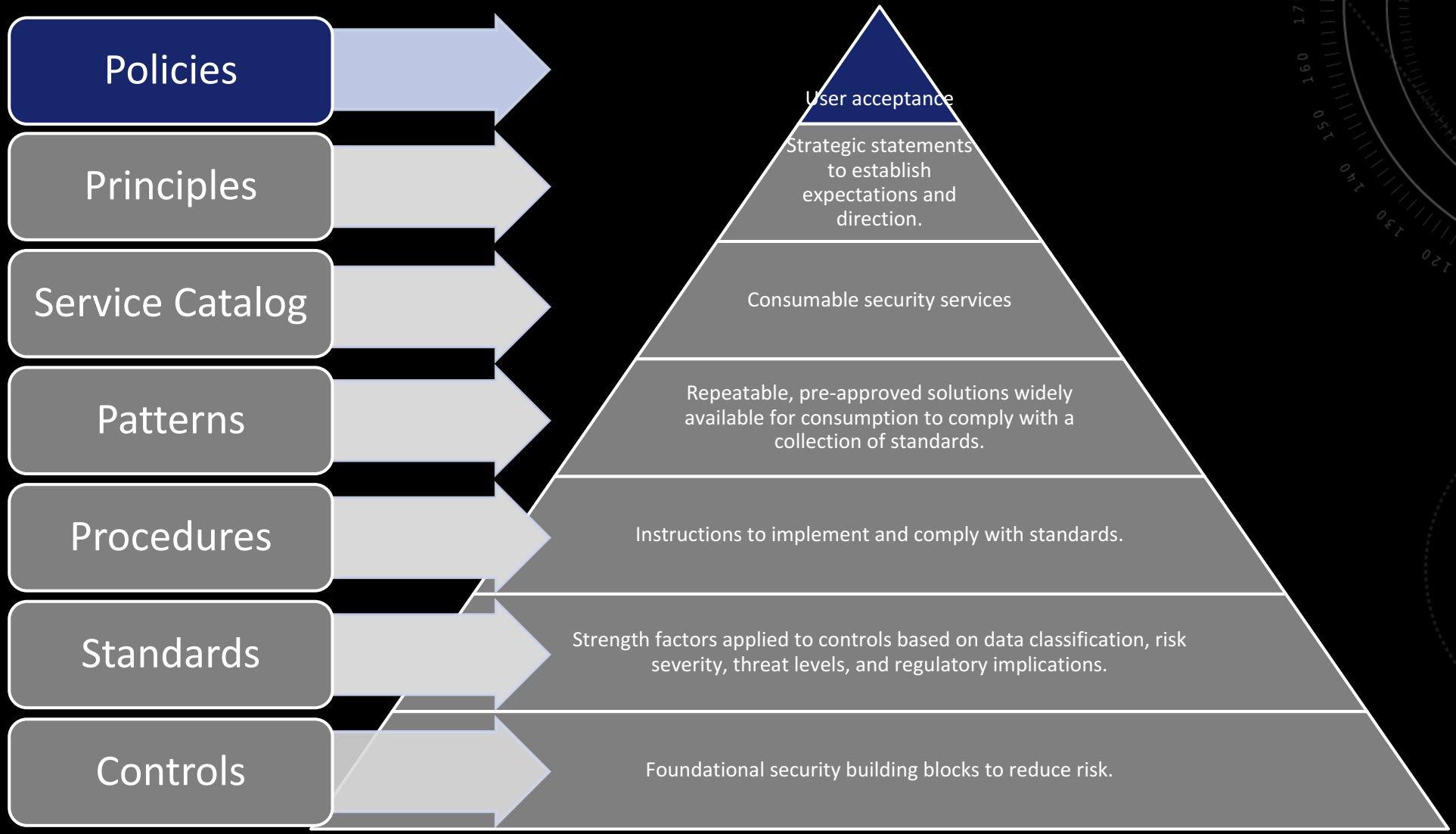
Architecture-at-scale



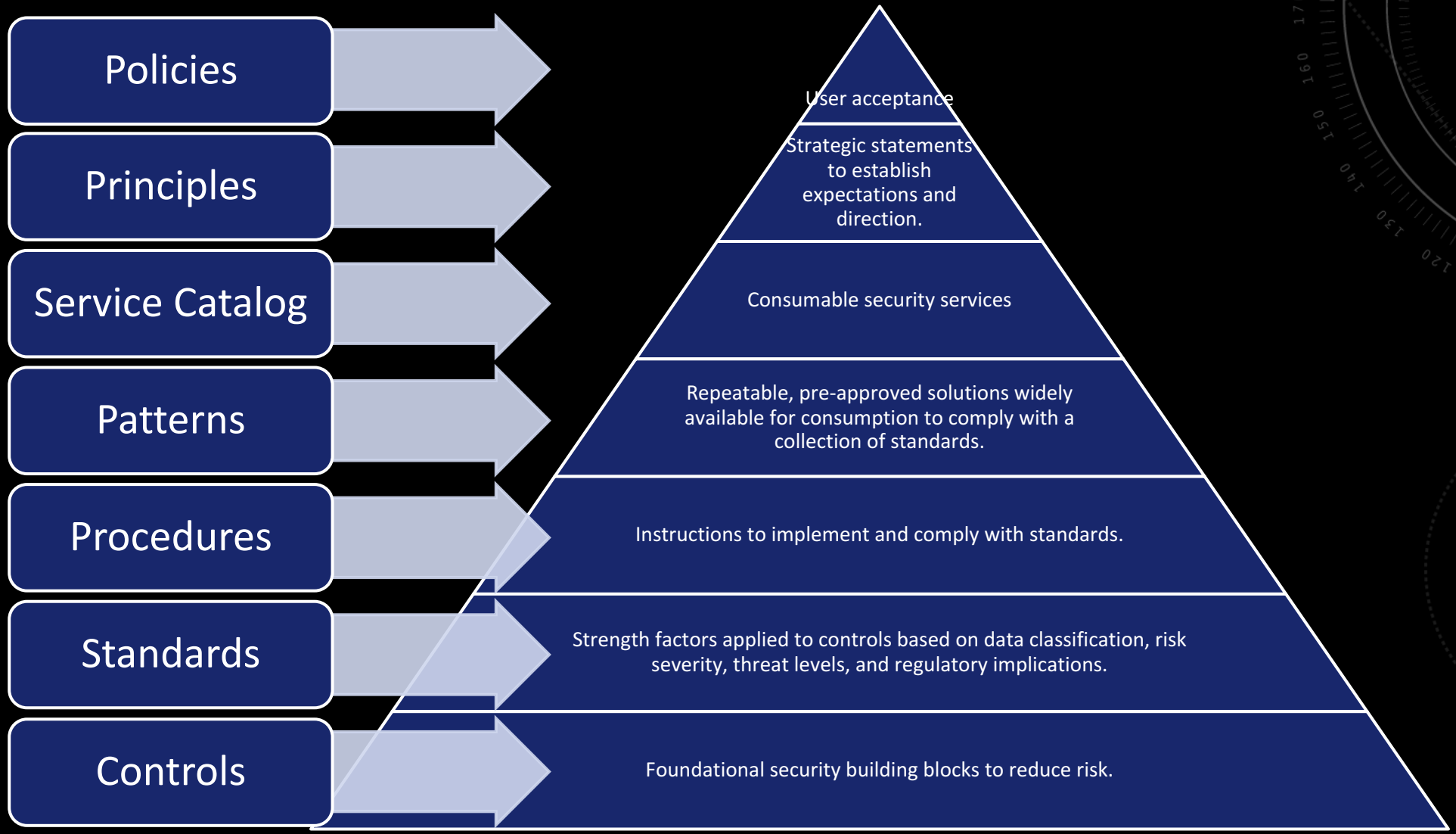
Architecture-at-scale



Architecture-at-scale



Architecture-at-scale



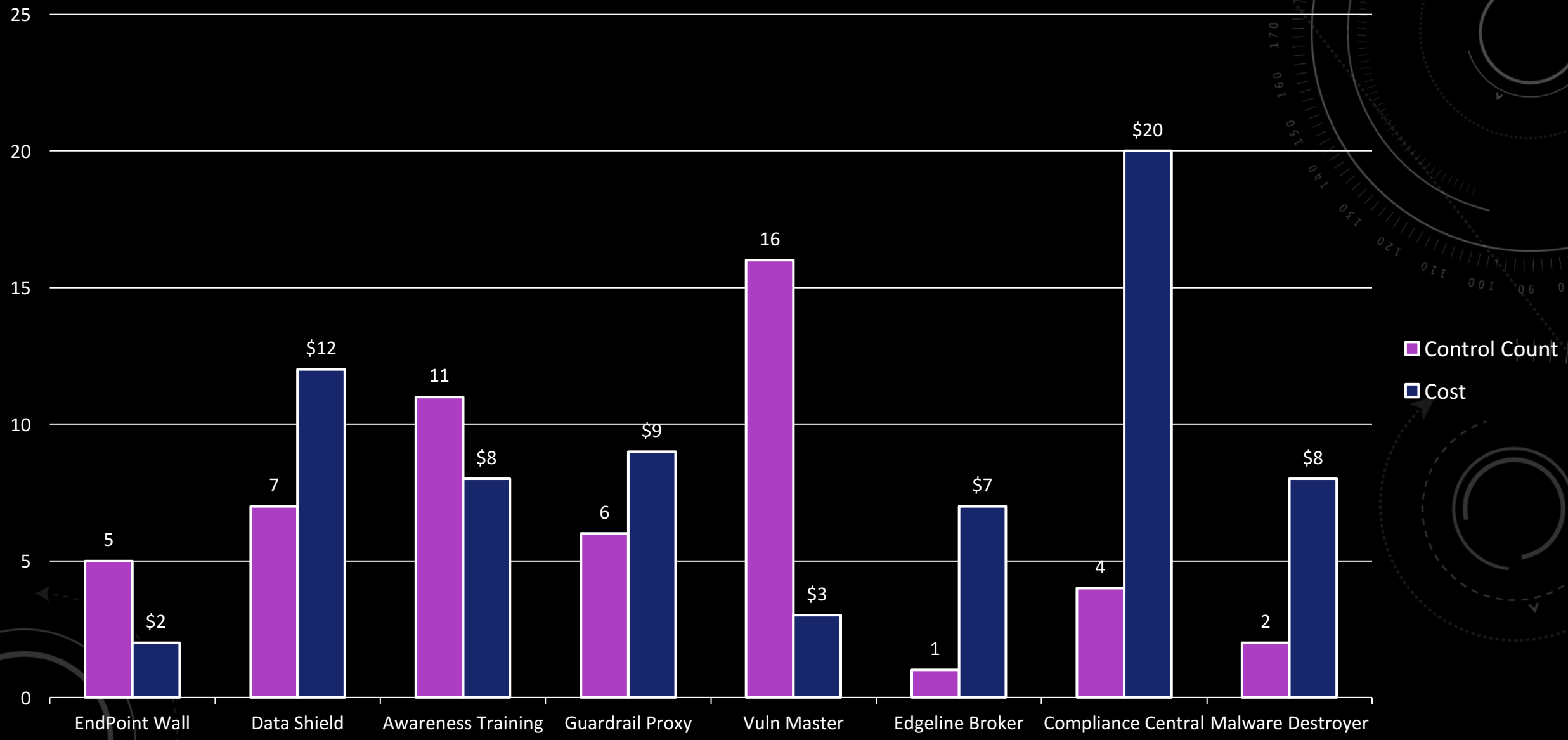
Example Artifacts

Phase 1 Control Catalog

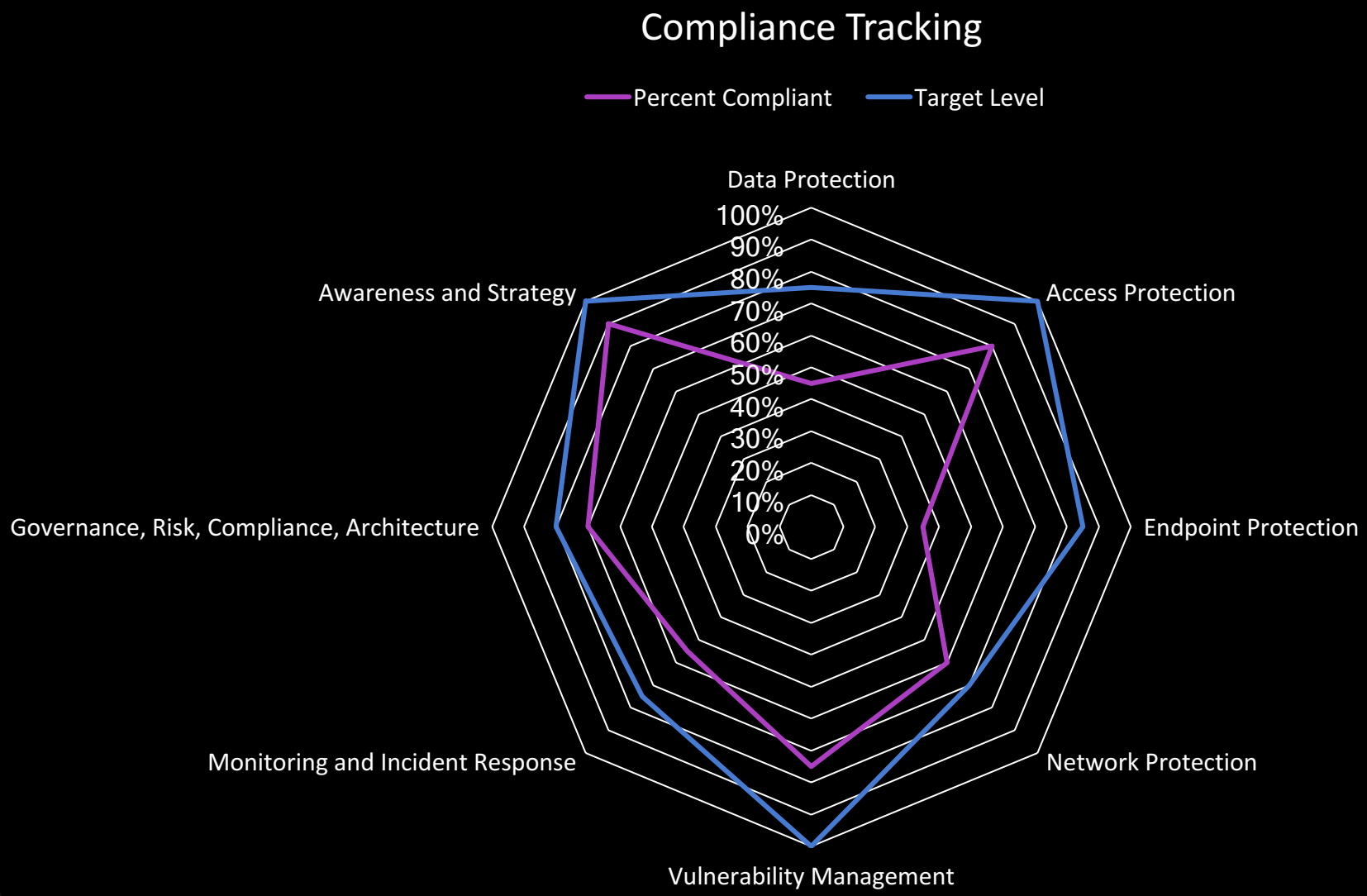
- Inventory and categorization of controls.
- Tracking the compliance of controls will highlight the utilized capabilities.
- Control mappings will formalize resource dependencies.

Ref #	Domain	Category	Control	Status
AC 1	Identity and Access Management	Authentication	Password policies must include length and complexity.	Core
SA 1	Awareness	Training	Users must not use email for non-business use.	Core
DS 1	Data Protection	Data Classification	Databases containing highly sensitive elements must be monitored.	Emerging
NS 1	Endpoint Security	Mobile	Mobile devices must be managed when accessing data.	Investigational

Cost benefit analysis.



Establish target goals.



Capture the program weaknesses.

- Evaluate the gaps against internal business risk.
- Analyze breaches and industry threats.
- Engage independent third-party assessors.
- Combine the information to develop a short-term and long-term strategy.

Plan for the needed capabilities.

- Balance the spend based on the risk.
- Invest in the program gaps.
- Align with the business strategy to plan for emerging risks.
- Determine the total cost of ownership for a short-term and long-term strategy.

Strategy distribution.

- Provide the overarching strategic capability goals across the leadership.
- Prioritize the focus.
- Develop tactical milestones and initiatives for completion taking into account people, process, and technology.
- Continually track execution status through delivery.
- Transition completed capabilities into ongoing governance.

Putting the pieces together.

1. Understand the business strategies.
2. Analyze the threat landscape.
3. Identify the existing program capabilities.
4. Determine what is most important to protect (the crown jewels).
5. Establish the program framework.
6. Map the controls to the capabilities.
7. Perform cost benefit analysis.
8. Set goal compliance targets.
9. Compile the short and long term strategy.
10. Develop the tactical milestones and track to completion.

Repeat this process annually.

A tool to help you succeed.

- Security Marker – securitymarker.io
  - Populate the data into pre-made spreadsheet.
  - Load the spreadsheet into the webpage.
  - Javascript will process the data and output D3.js visualizations.
  - Everything stays completely client side so no sensitive data is transmitted.

Thank you!

Contact Information

ryan-elkins@outlook.com

Twitter: @the_ryan_elkins