Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

Shifting Left on Governance

Public Sector Network

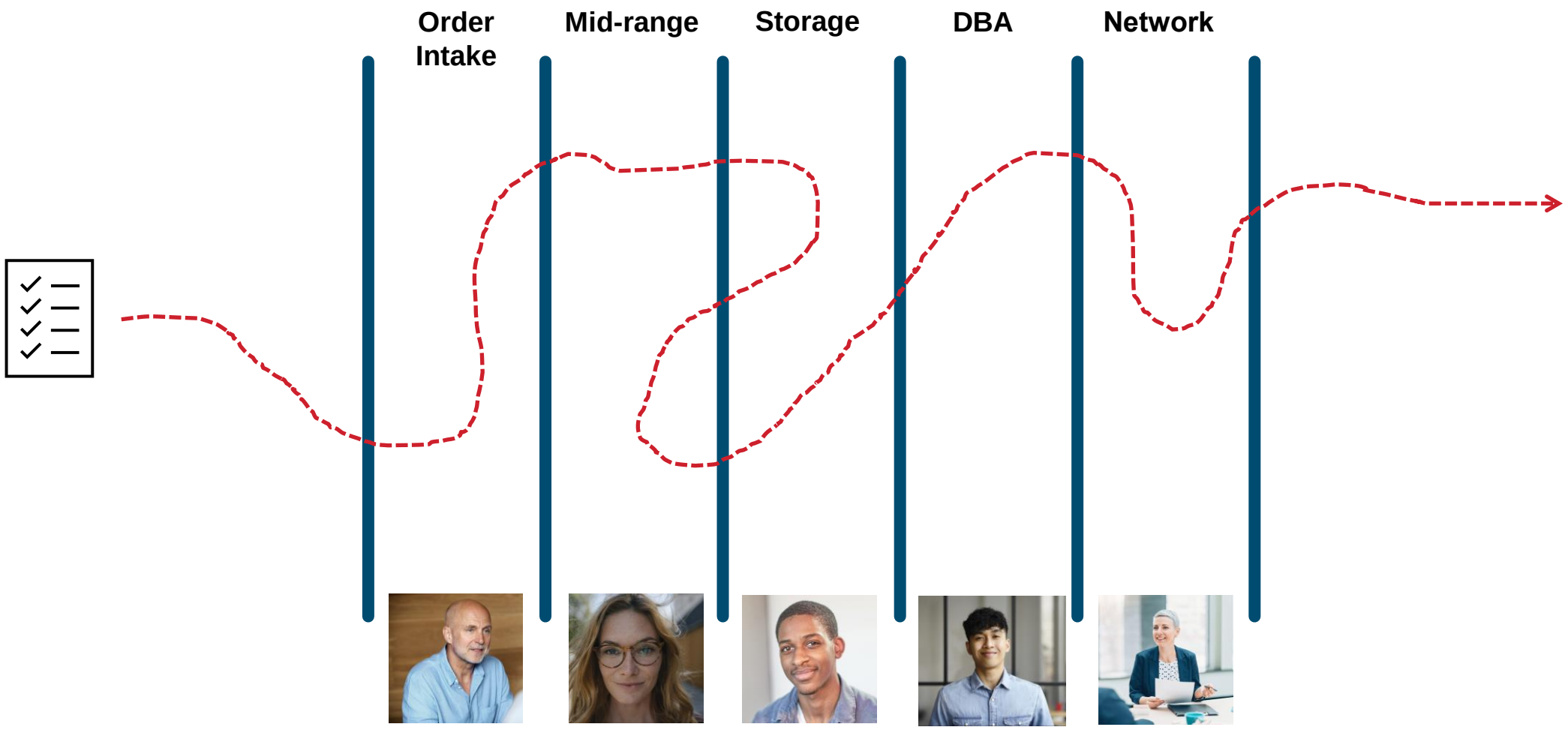
Scott N. Levac

@scottnlevac

GC's Cloud Adoption Journey

A policy wonk's view

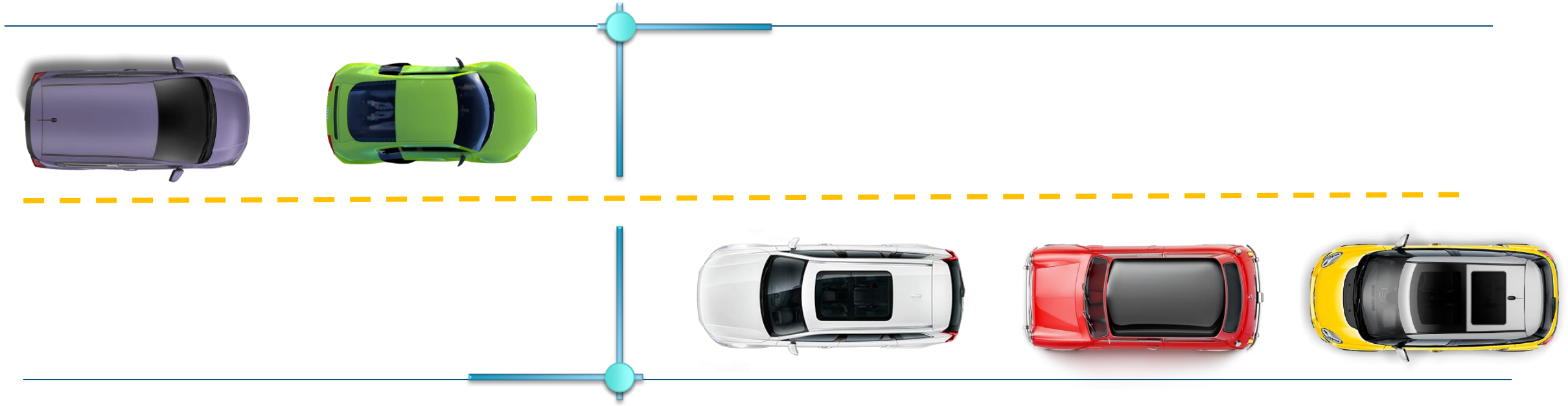
Traditional Governance - Artisanal



Two Delivery Models – Different Attributes

	 **Traditional**	 **Public Cloud**
Provisioning Model	Order Intake	APIs
Organizational Structure	Functional	Delivery
Delivery Frequency	Periodic	Continuous
Governance Model	Gates	?

Avoid Governing With Gates



- Brings activity to a halt
- Requires a gatekeeper to arbitrate on pass/fail
- Criteria for pass/fail can be misunderstood

How To Make Everyone Happy?

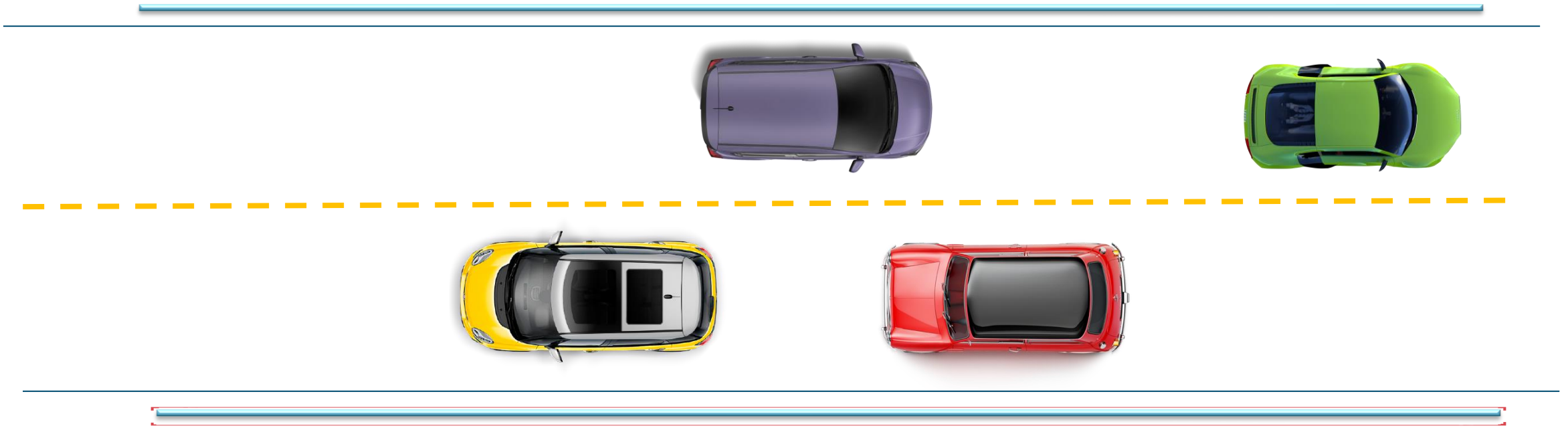
C-Suite Executives

"I want to make sure nothing high-risk is happening"

Delivery Teams

"I want to make my users happy by delivering new features"

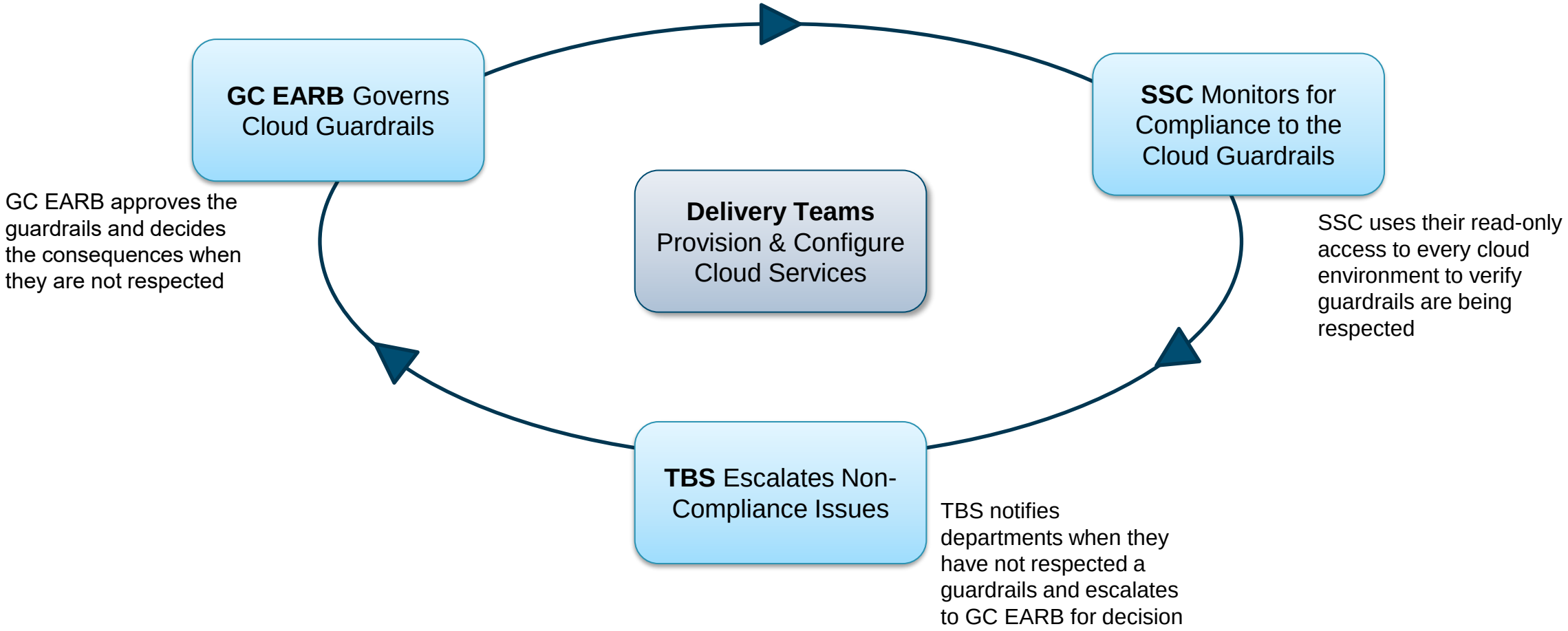
Govern With Guardrails



- Keeps activities flowing
- Defined, coded, limits to pass/fail
- Telemetry collected for guardrail violations

Governing by Guardrails: Centralized Visibility, Delivery Team Agility

A ***trust, but verify model*** is used: departments are trusted to safely operate their cloud accounts, but the enterprise has the ability to verify their usage. Rather than a traditional gating governance, a guardrails approach to governance was implemented. As long as guardrails are respected, departmental delivery teams can keep using the self-service features of cloud uninterrupted.



What Are Our Guardrails?

- Protect root / global admins account
- Management of administrative privileges
- Cloud console access
- Enterprise monitoring accounts
- Data location
- Protection of data-at-rest
- Protection of data-in-transit
- Segment and separate
- Network security services
- Cyber defense services
- Logging and monitoring
- Configuration of cloud marketplaces

https://github.com/canada-ca/cloud-guardrails

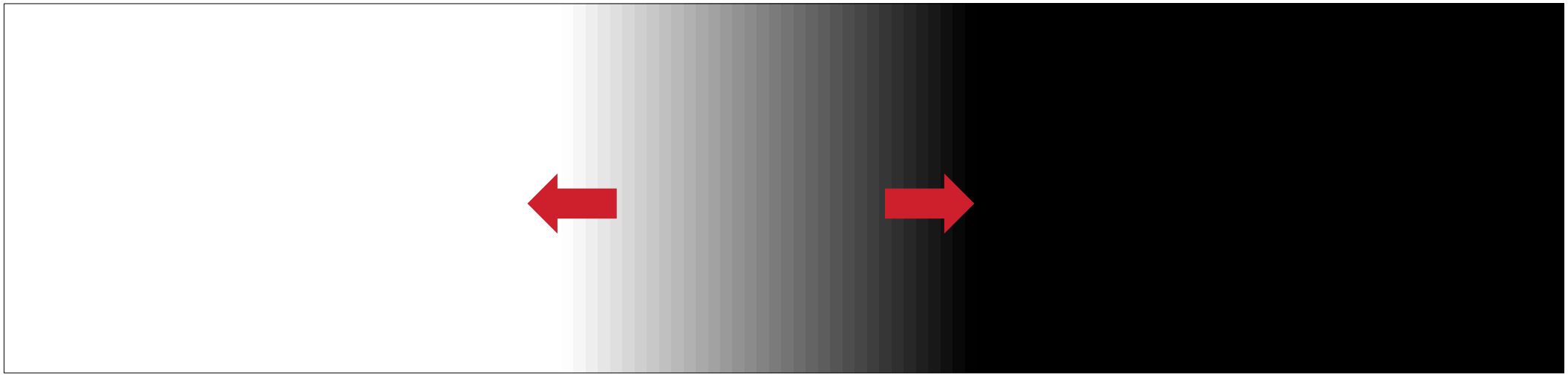
Shifting Left – Eliminating Shades of Grey

Remove the grey, drive towards black or white.

Things that are allowed

Ambiguity

Things that are not allowed



Source: AWS re:Invent 2018: The Tension Between Absolutes & Ambiguity in Security (SEC310) - YouTube

What Does Shifting Left on Governance Mean?