Regulations and Standards for Confidential Computing

Mike Bursell
Executive Director, CCC

CONFIDENTIAL COMPUTING CONSORTIUM

Abstract

- Industry recognition of Confidential Computing has risen significantly and there is availability in public and private clouds: what is next? One of the ways to drive demand for CC solutions is via regulations and standards. This session introduces some of the ways this is happening and discusses some of the options for the future - and ways for individuals and organisations to get involved.

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

The Confidential Computing Consortium
Why regulations and standards?
Regulations
Standards
The work of the CCC

CONFIDENTIAL COMPUTING CONSORTIUM

The Confidential Computing Consortium

The CCC

“The Confidential Computing Consortium (CCC) brings together hardware vendors, cloud providers, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards.”

CONFIDENTIAL COMPUTING CONSORTIUM

The CCC

“The Confidential Computing Consortium (CCC) brings together hardware vendors, cloud providers, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards.”

CONFIDENTIAL COMPUTING CONSORTIUM

The CCC

“The Confidential Computing Consortium (CCC) brings together hardware vendors, cloud providers, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards.”

If you’re here
or watching online then …

CONFIDENTIAL COMPUTING CONSORTIUM

The CCC

“The Confidential Computing Consortium (CCC) brings together hardware vendors, cloud providers, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards.”

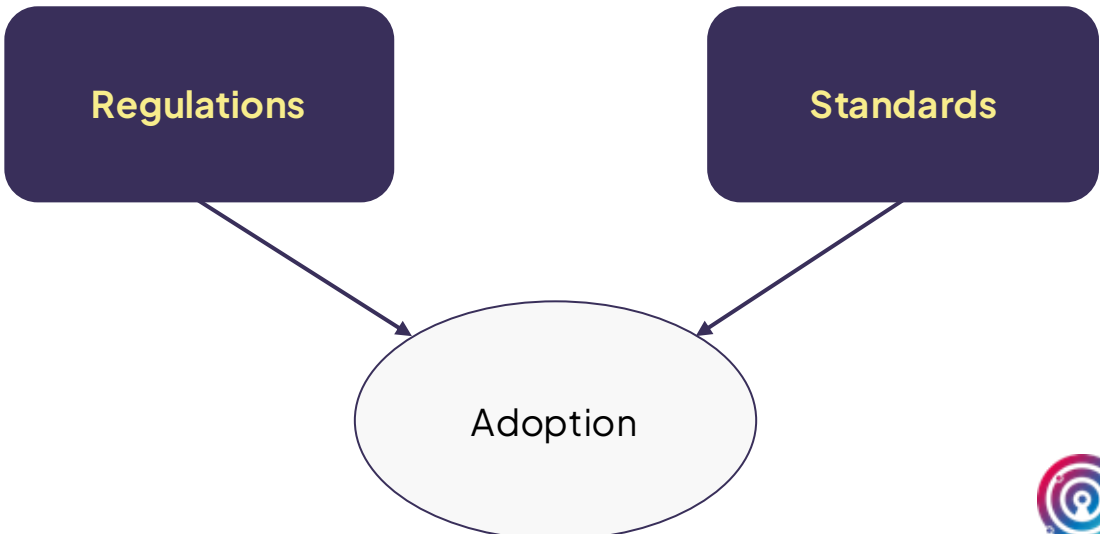
If you’re here
or watching online then …
…your organisation should probably be a member!

CONFIDENTIAL COMPUTING CONSORTIUM

Why regulations and standards?

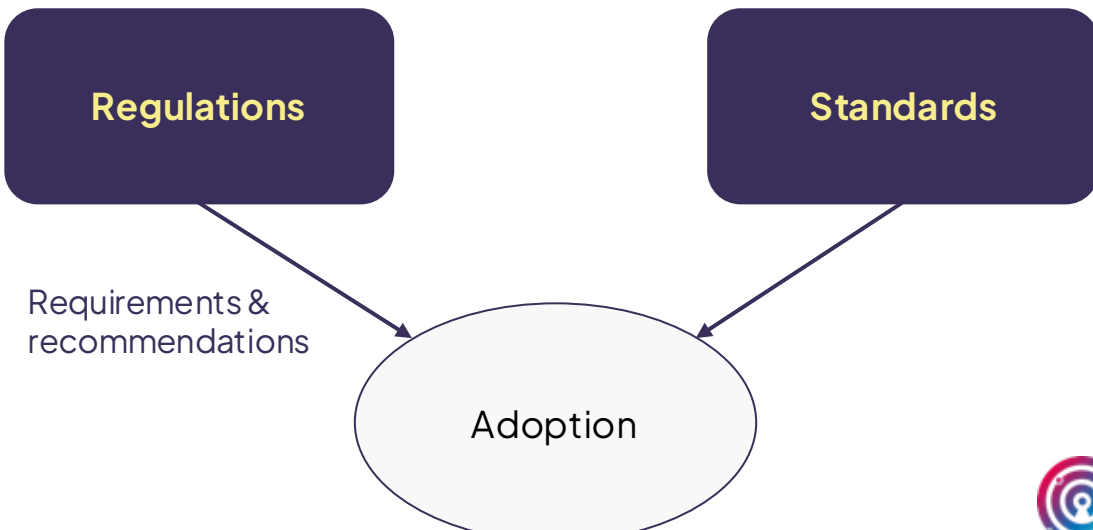
CONFIDENTIAL COMPUTING CONSORTIUM

Why regulations and standards?



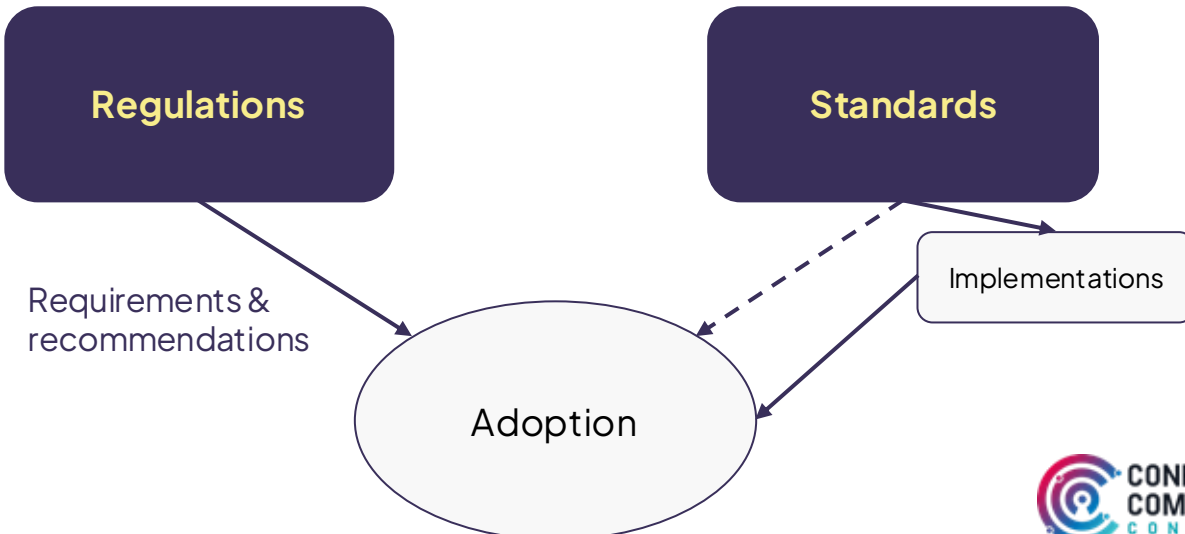
CONFIDENTIAL COMPUTING CONSORTIUM

Why regulations and standards?



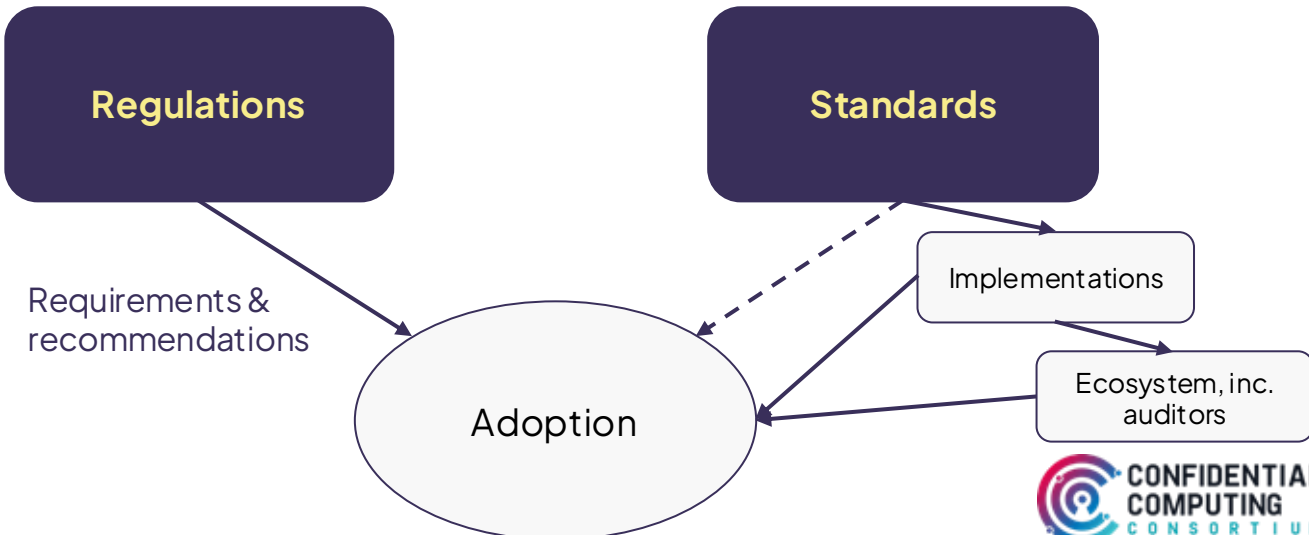
CONFIDENTIAL COMPUTING CONSORTIUM

Why regulations and standards?



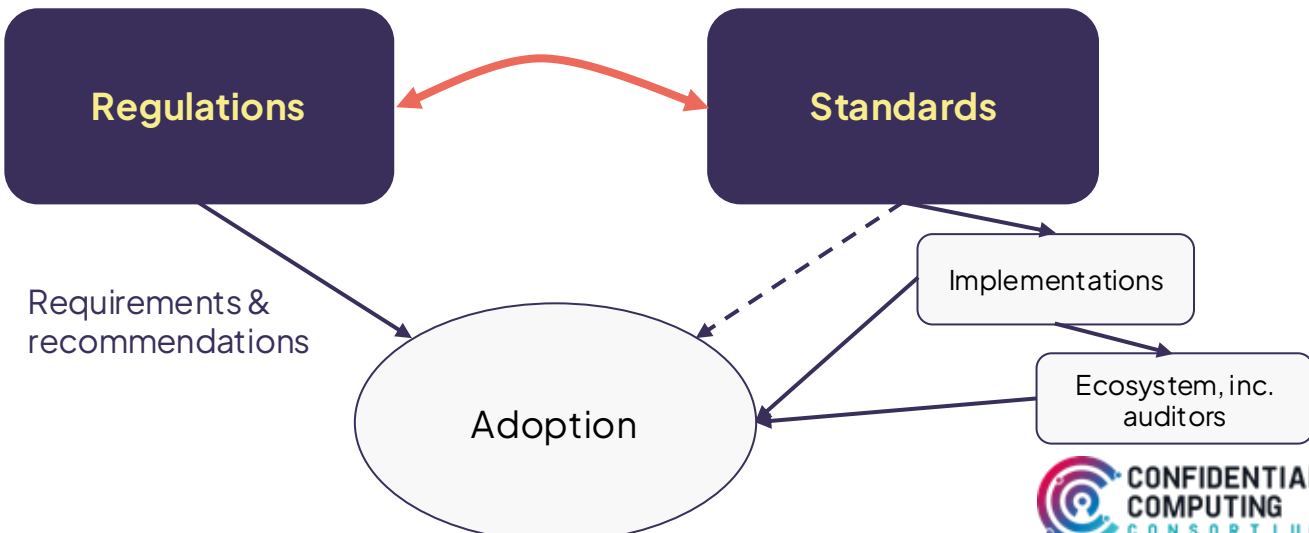
CONFIDENTIAL COMPUTING CONSORTIUM

Why regulations and standards?



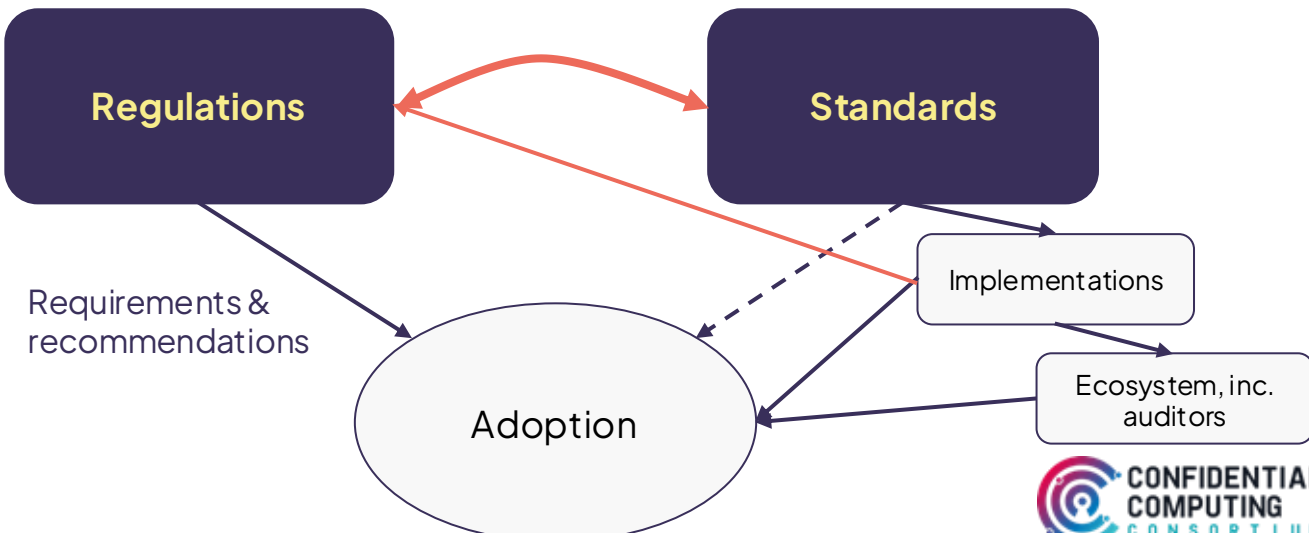
CONFIDENTIAL COMPUTING CONSORTIUM

Why regulations and standards?



CONFIDENTIAL COMPUTING CONSORTIUM

Why do regulations and standards matter to us?



CONFIDENTIAL COMPUTING CONSORTIUM

Regulations & Regulators

CONFIDENTIAL COMPUTING CONSORTIUM

Regulators

National bodies (e.g. BSI, ANSSI, ANSI, FDA, Singapore MAS, UK-PRA)
International bodies (e.g. ISO, PCI-SSC)
Sector-specific (e.g. EBA, ESMA)

Typically move slowly

- except in response to specific events
  - "knee-jerk" regulations* can be flawed!

*particularly those which which point at standards

CONFIDENTIAL COMPUTING CONSORTIUM

Regulators

Mostly **MUST** - but start with **SHOULD**

Often require technical standards in place - otherwise how can they enforce?

CONFIDENTIAL COMPUTING CONSORTIUM

Specific areas CC interest

Financial
Digital Sovereignty
Agentic AI
Web3 (+ cryptocurrencies?)
Data privacy (e.g. GDPR)
Healthcare
National Security
?AI

CONFIDENTIAL COMPUTING CONSORTIUM

Specific areas CC interest

Financial
Digital Sovereignty
Agentic AI
Web3 (+ cryptocurrencies?)
Data privacy (e.g. GDPR)
Healthcare
National Security
?AI

Considerable overlap between these!

CONFIDENTIAL COMPUTING CONSORTIUM

Standards & Standards Bodies

Standards and standards bodies

Regulations easier to drive with standards

Some key bodies:

- IETF - network protocols

CONFIDENTIAL COMPUTING CONSORTIUM

Standards and standards bodies

Regulations easier to drive with standards
Some key bodies:

- IETF - network protocols
- W3C - application-layer

CONFIDENTIAL COMPUTING CONSORTIUM

Standards and standards bodies

Regulations easier to drive with standards
Some key bodies:

- IETF - network protocols
- W3C - application-layer
- ISO - “safety, quality, and efficiency across industries”

CONFIDENTIAL COMPUTING CONSORTIUM

Standards and standards bodies

Regulations easier to drive with standards
Some key bodies:

- IETF - network protocols
- W3C - application-layer
- ISO - “safety, quality, and efficiency across industries”
- NIST - officially USA; strong security history

NIST

CONFIDENTIAL COMPUTING CONSORTIUM

Standards and standards bodies

Regulations easier to drive with standards

Some key bodies:

- IETF - network protocols
- W3C - application-layer
- ISO - “safety, quality, and efficiency across industries”
- NIST - officially USA; strong security history
- ETSI (telecommunications)

CONFIDENTIAL COMPUTING CONSORTIUM

Standards and standards bodies

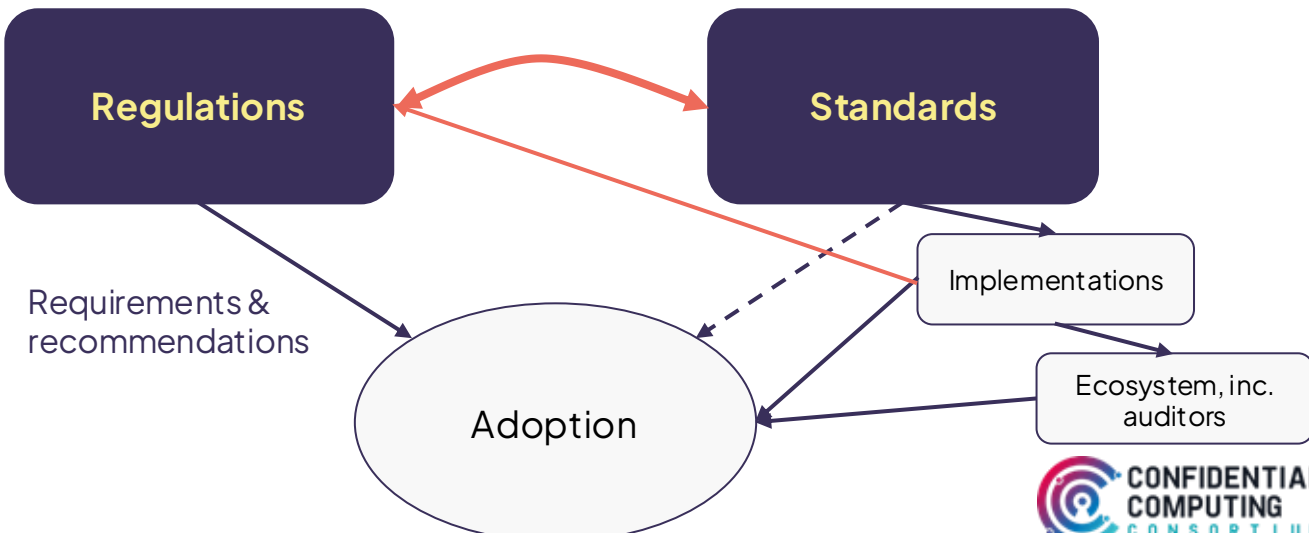
Regulations easier to drive with standards
Some key bodies:

- IETF - network protocols
- W3C - application-layer
- ISO - “safety, quality, and efficiency across industries”
- NIST - officially USA; strong security history
- ETSI (telecommunications)
- ANSSI (also a regulatory body)

Question: who are we trying to influence or help?

CONFIDENTIAL COMPUTING CONSORTIUM

Why do regulations and standards matter to us?



CONFIDENTIAL COMPUTING CONSORTIUM

Technical standards – areas

Some of the areas

- Protocols
  - Networking
  - Storage
  - Key exchange
- Attestation
- Multiple TEEs (e.g. TDISP)
- Cross-system TEEs (beyond TDISP)
- TEE integration

CONFIDENTIAL COMPUTING CONSORTIUM

“What is a CC-enabled app?”

Presumably…

- an application (or service)
- that meets the CCC’s definition of Confidential Computing
  - making use of hardware-based TEEs
  - making use of remote attestation
- **maybe** using particular protocols
- BUT…

CONFIDENTIAL COMPUTING CONSORTIUM

“What is CC?”

BUT…

- We don’t have a formal technical definition of a hardware-based TEE
- And we have lots of attestation mechanisms

This needs definition!
“Confidential Computing Assurance Framework”?

CONFIDENTIAL COMPUTING CONSORTIUM

“What is CC?”

BUT…

- We don’t have a formal technical definition of a hardware-based TEE
- And we have lots of attestation mechanisms

This needs definition!
“Confidential Computing Assurance Framework”?

CONFIDENTIAL COMPUTING CONSORTIUM

The work of the CCC

What's most important?

Lots of interdependencies across standards

- Hierarchies of protocols and models …
- … therefore of standards

CONFIDENTIAL COMPUTING CONSORTIUM

What's most important?

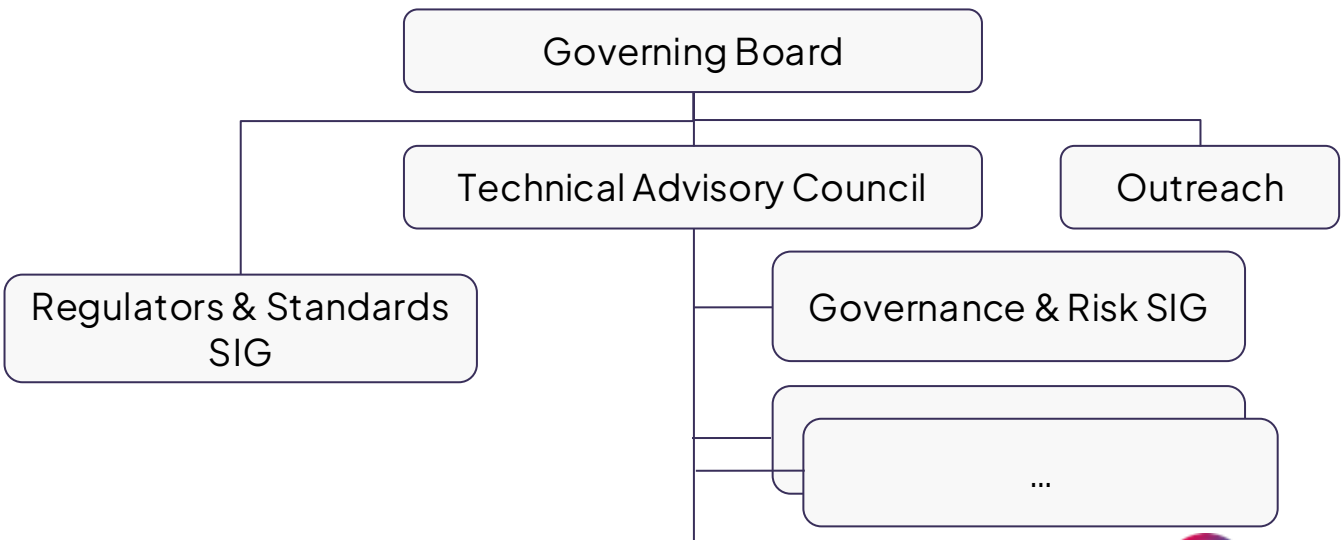
Lots of interdependencies across standards

- Hierarchies of protocols and models …
- … therefore of standards

We need to identify key priorities & bodies and then engage with them

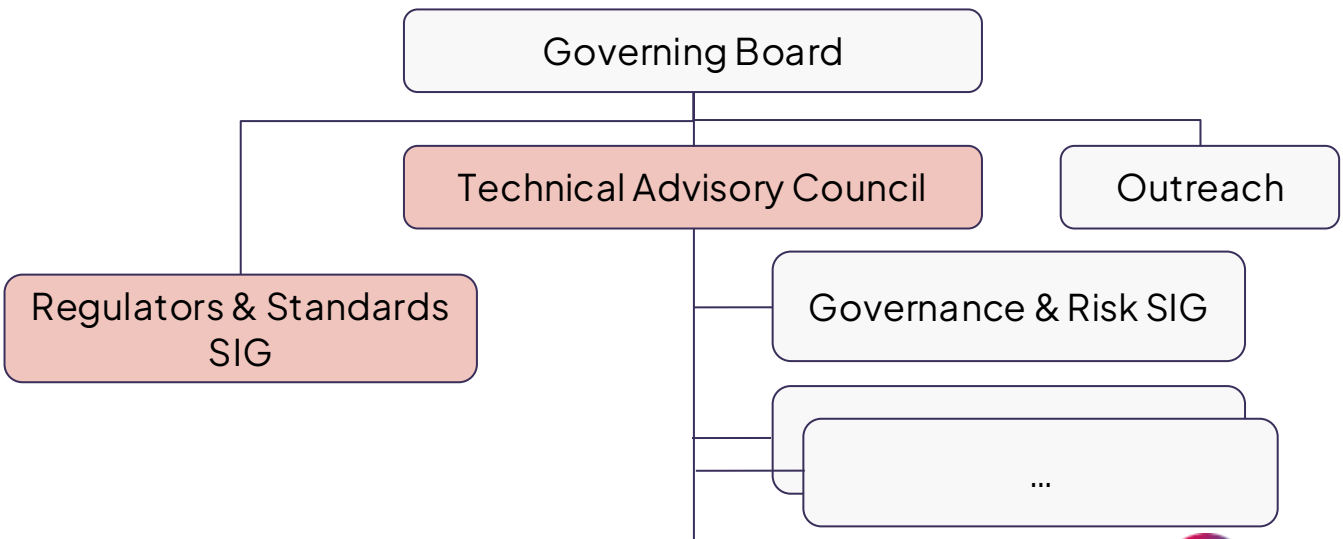
CONFIDENTIAL COMPUTING CONSORTIUM

CCC committees & SIGS



CONFIDENTIAL COMPUTING CONSORTIUM

CCC committees & SIGS



CONFIDENTIAL COMPUTING CONSORTIUM

CCC – getting involved

You don’t need to be a member to participate

We don’t just need tech experts

CONFIDENTIAL COMPUTING CONSORTIUM

CCC – getting involved

You don’t need to be a member to participate

We don’t just need standards experts

CONFIDENTIAL COMPUTING CONSORTIUM

CCC – getting involved

You don’t need to be a member to participate

We don’t just need law experts

CONFIDENTIAL COMPUTING CONSORTIUM

CCC – getting involved

You don’t need to be a member to participate

We need [tech|standards|law] experts

CONFIDENTIAL COMPUTING CONSORTIUM

CCC – getting involved

You don't need to be a member to participate
We need [tech|standards|law] experts

TAC + Regs & Standards SIG

- https://confidentialcomputing.io/about/committees/
- Email lists
- Slack channels
- Meetings every two weeks (fortnightly)

CONFIDENTIAL COMPUTING CONSORTIUM

Questions