# Can IoT security risk management be made simple?

26th November 2019

Paul Kearney

Professor of Cybersecurity, Birmingham City University

paul.kearney@bcu.ac.uk

# Disclaimer

The thoughts presented here are personal views arising while working on the IoTSF Compliance Class Determination guidance report, which is very much still work in progress.

# Reconciling conflicting viewpoints

The demand for the benefits IoT can offer is high, but security is widely recognized as a concern.

- Question from IoT end user or developer:
  - Is this device/system secure?
  - How do I make this device/system secure?
- Reply from security professional:
  - Well, I'll need to do a risk assessment to answer that!

*The questioner wants a simple, prescriptive, objective answer, but security is complex, context-dependent and subjective!*

# Two stakeholder perspectives

Customer / end-user

Product

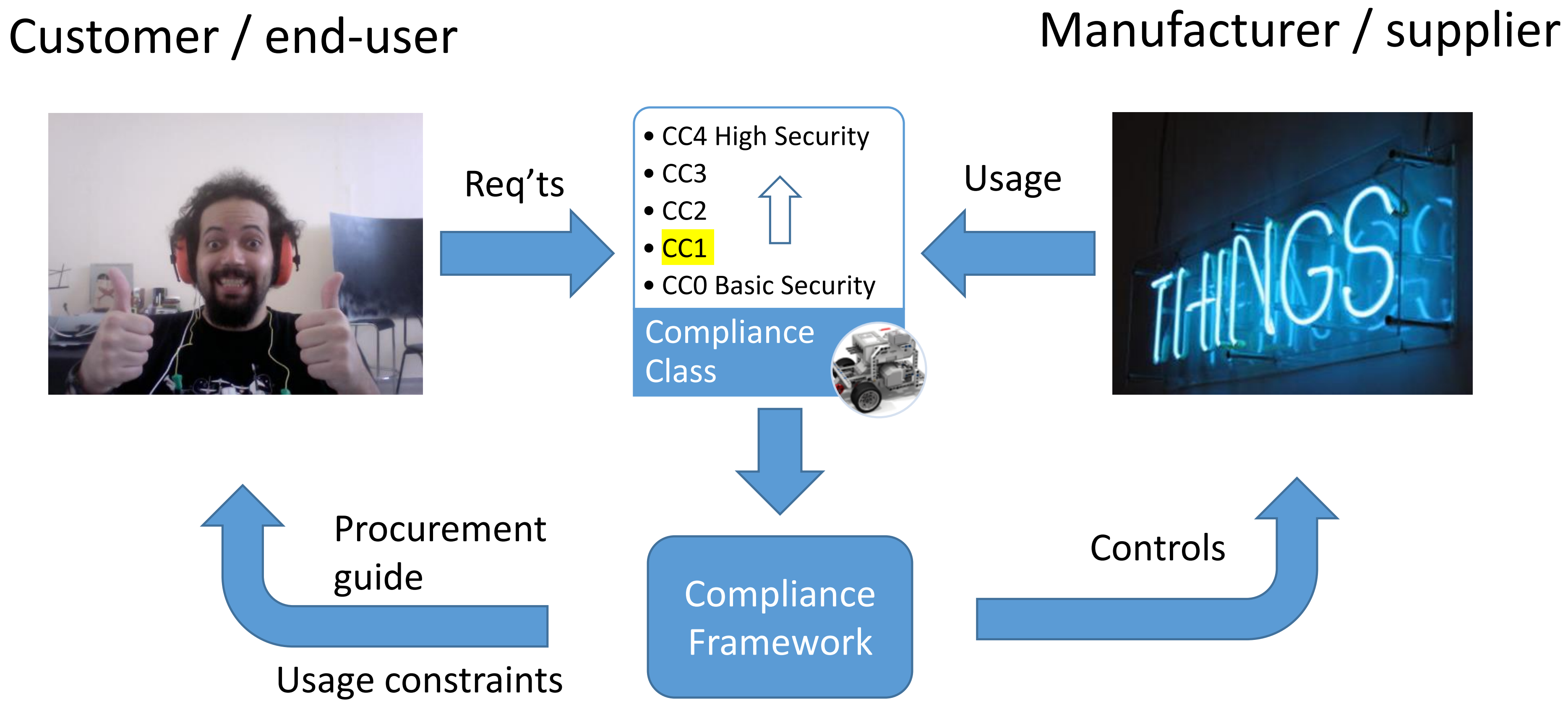
Target of evaluation (ToE)

Manufacturer / supplier

| | |
|---|---|
| Knows: | • Where, for what and how the product will be used |
| Wants to know: | • Which product to buy<br>• How to use it securely |
| Doesn't know | • Innards of product<br>• About security |

| | |
|---|---|
| Knows: | • All about the product |
| Wants to know: | • Product is secure enough for its market?<br>• Limitations on secure usage |
| Doesn't know | • Usage environment<br>• About security |

# IoTSF: Introducing the Compliance Class



Customer / end-user

Manufacturer / supplier

Req'ts

- CC4 High Security
- CC3
- CC2
- CC1
- CC0 Basic Security

Compliance Class

Usage

Compliance Framework

Procurement guide

Usage constraints

Controls

# Security risk management (SRM)

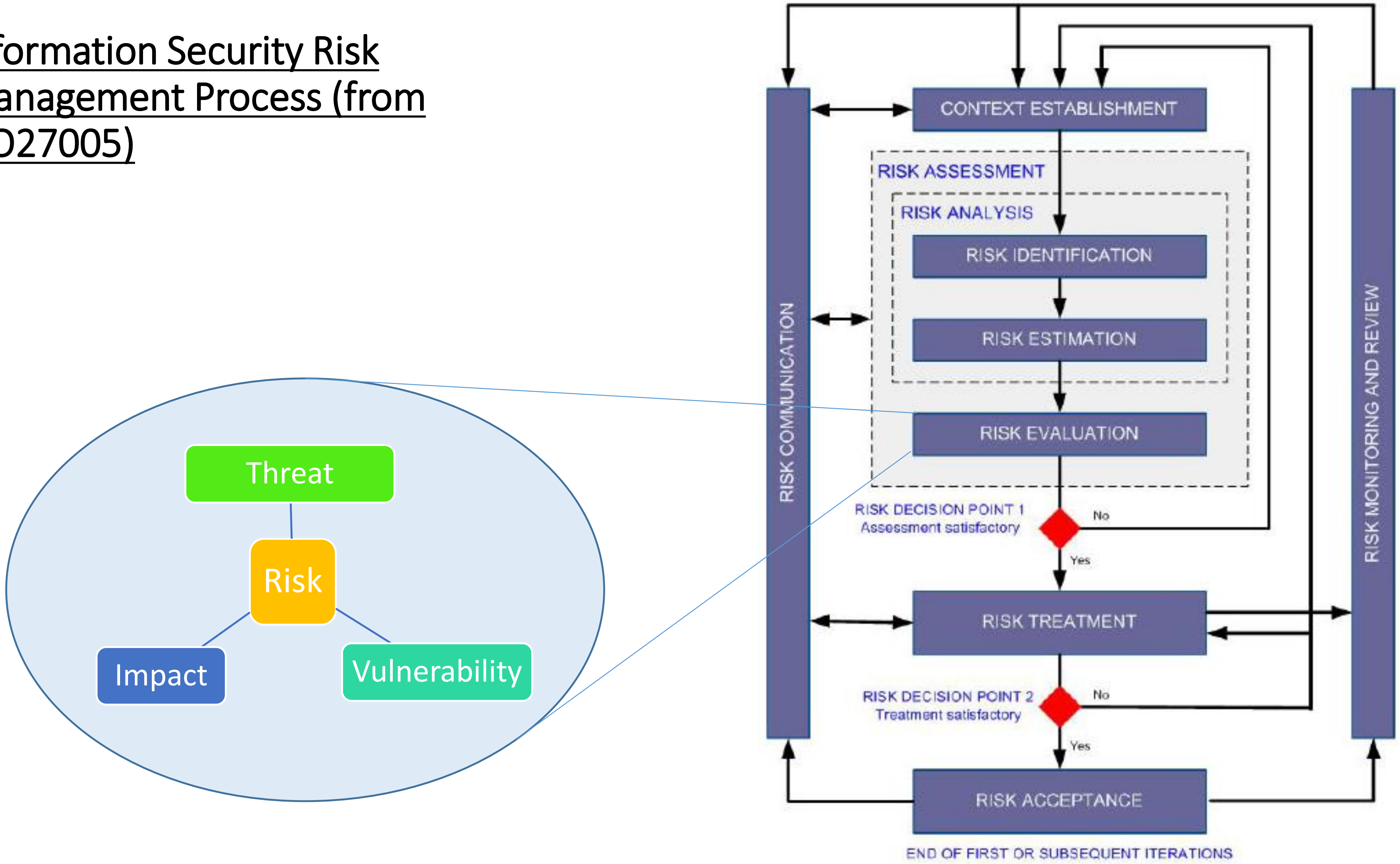
- SRM is about balancing Risk Exposure against Risk Appetite
- Risk appetite is an attribute of the system owner
- Risk exposure depends on:
  - Dependency of assets on the ToE (Impact)
  - Exposure to threat agents
  - Vulnerability of ToE

Properties of environment

Property of ToE

**Theory**:
If we choose the ‘right’ compliance class and the ToE satisfies the Compliance Framework, then Risk Exposure and Risk Appetite ***should*** be in balance.

# Information Security Risk Management Process (from ISO27005)



Threat

Risk

Impact

Vulnerability

CONTEXT ESTABLISHMENT

RISK ASSESSMENT

RISK ANALYSIS

RISK IDENTIFICATION

RISK ESTIMATION

RISK EVALUATION

RISK DECISION POINT 1
Assessment satisfactory

No

Yes

RISK TREATMENT

RISK DECISION POINT 2
Treatment satisfactory

No

Yes

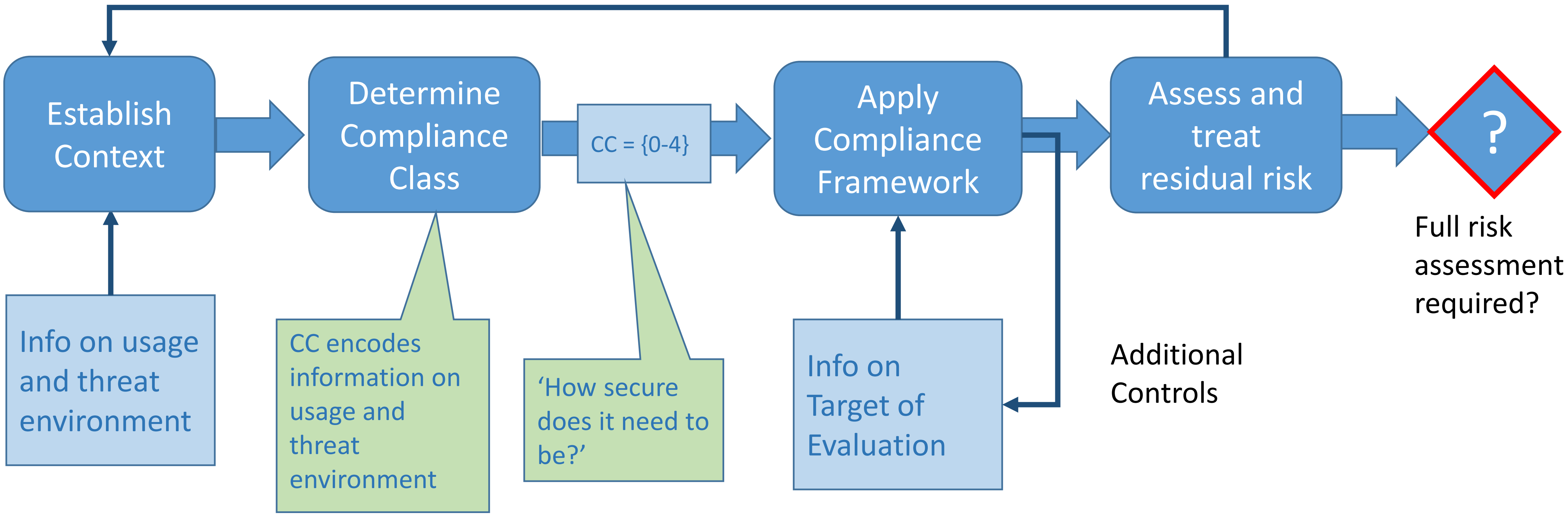
RISK ACCEPTANCE

END OF FIRST OR SUBSEQUENT ITERATIONS

RISK COMMUNICATION

RISK MONITORING AND REVIEW

# Extended Compliance Process



Establish Context

Determine Compliance Class

CC = {0-4}

Apply Compliance Framework

Assess and treat residual risk

?

Full risk assessment required?

Info on usage and threat environment

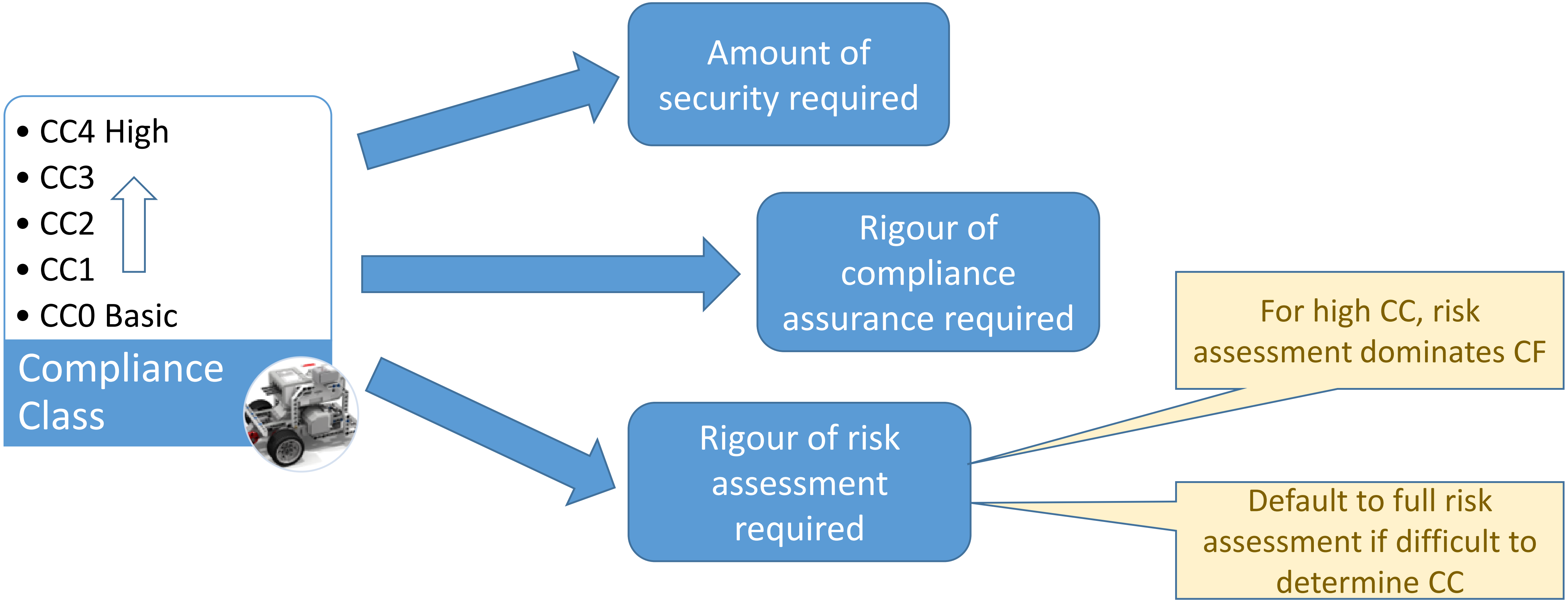
CC encodes information on usage and threat environment

'How secure does it need to be?'

Info on Target of Evaluation

Additional Controls

# The Compliance Class concept is overloaded



- CC4 High
- CC3
- CC2
- CC1
- CC0 Basic

Compliance Class

Amount of security required

Rigour of compliance assurance required

Rigour of risk assessment required

For high CC, risk assessment dominates CF

Default to full risk assessment if difficult to determine CC

# Summary and conclusions

- Seeking middle way between prescriptive and principles-based approaches to IoT security.
- Embed IoTSF Compliance Framework within Risk Management process
  - Compliance Class + Framework should result in acceptable risk exposure
  - Still need to assess residual risk and treat if necessary
- Educate end-users and developers in principles of risk management
  - CC determination is not trivial, even for low classes
  - Still need full risk assessment for higher CC and where classification is uncertain