

1

## System of interest

Pick a system or component of interest. It should be something that matters to everyone in the group. Write its name at the top of the board.

2

## Key Security Claim

Discuss what security claim associated with the system of interest matters most to the group. Write it at the top of the board.

1

## Recommendation

Who recommended the system? Add them to the board.

2

## Vendor

Who was the system purchased from? Add them to the board.

3

## Security

Who defined the security model for the system? Add them to the board.

4

## Design

Who designed the system and/or its implementation? Add them to the board (if not there already)

5

## Manufacture

Who made the system? Add them to the board (if they are not there already)

6

## Components

Are there component parts of the system made by other vendors? Add any key suppliers/supply chain parties to the board.

7

## Configuration

Who is responsible for configuring the system? Add them to the board.

8

## Test

Who has tested the system? Add them to the board (if they are not already there)

9

## Accountability

Who is accountable for the security of the system? Add them to the board.

10

## Maintenance

Who operates and maintains the system? Add them to the board.

11

## Standards

Does the system have to meet any key standards or criteria? If so, who sets the standards? Add them to the board.

12

## Regulation

Are there regulators who have a specific interest in the system? Add them to the board.

1



## Test reports

Consider test completion reports, such as user acceptance, as well as security specific reports such as from a penetration testing exercise.

2



## Design documents

Specifications exist on many levels, from architectural documentation specific to the implementation, to design documentation for products used.

3



## Audit reports

Consider internal audit reports and external audit reports.

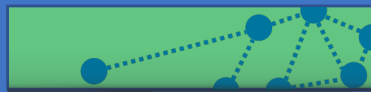
4



## Approvals

Consider how approvals are documented, and how records are shared.

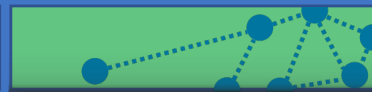
5



## Certificates

Is the system certified in any way? Certification may be carried out by a 'third party' or by an internal authority.

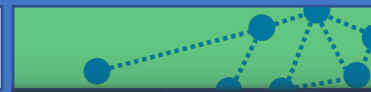
6



## Word of Mouth

Some of the most consequential knowledge about the security of systems is not found in formal reports. Consider what is shared by word of mouth.

7



## Familiarity

Personal experience or learned expertise, forms of knowledge that belong to individuals, and move with them between organisations rather than being written down.

8



## Witnessing

Consider the role of direct observation or witnessing (for instance of a supplier's facilities or working practices)

9



## Other texts

Any other texts missing from  
the cards that matter to the  
security of the system.

1



## Events

How have particular events (such as breaches, incidents, interventions) changed the shape of the diagram? Annotate as appropriate.

2



## Intervention

Go round the group. On the map, what is one thing that you would like to change in order to make things better? Annotate as appropriate.

3



## Policy

Go round the group. In what areas is there a need for policy interventions? For instance, regulation, new standards, guidance, third party reports, or new certification schemes.

4



## Uncertainty

Which parts of the diagram are you most certain about? Which parts are you most uncertain about? Annotate as appropriate.

5



## Visibility

Which nodes have the greatest visibility? Which have the least? Does it help or hinder assurance?

6



## Communication

Which nodes on the map share a common language and which struggle to communicate?