

KEEP

- Evidence

define priorities vs preservation

- Levels

What are they?

- Tools

- Comms/collab

- Capabilities/role

(Not too many people in meetings!)

- Kan-Ban Cards

- Role cards inc desc.
- Incident process

Infosec vs Service Incident - tips

Option 1

- Start with all roles relevant to ^{all types of} incidents involved
- Teams/roles drop out if not relevant to them.

Option 2

- One service desk team gets all reports. They do the verification & pass to correct team to manage incident

NB: sec incident may have less clear impact.
sec incident may not be aiming for quick restore