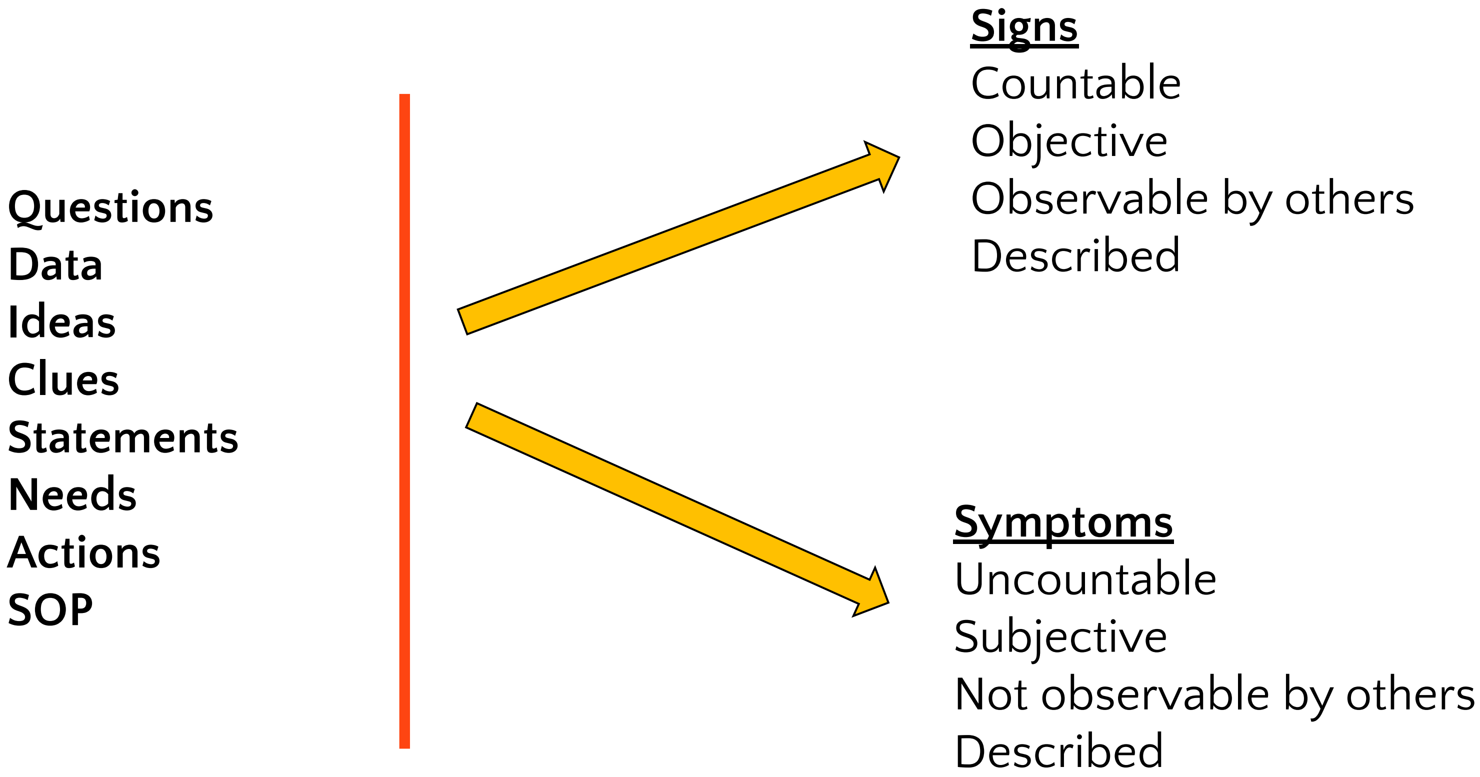
OnSite
Incident Management Training

Operational Period #3

Breakout session #2

© 2022 V1 Blackrock 3 Partners, Inc.

Incident Documentation



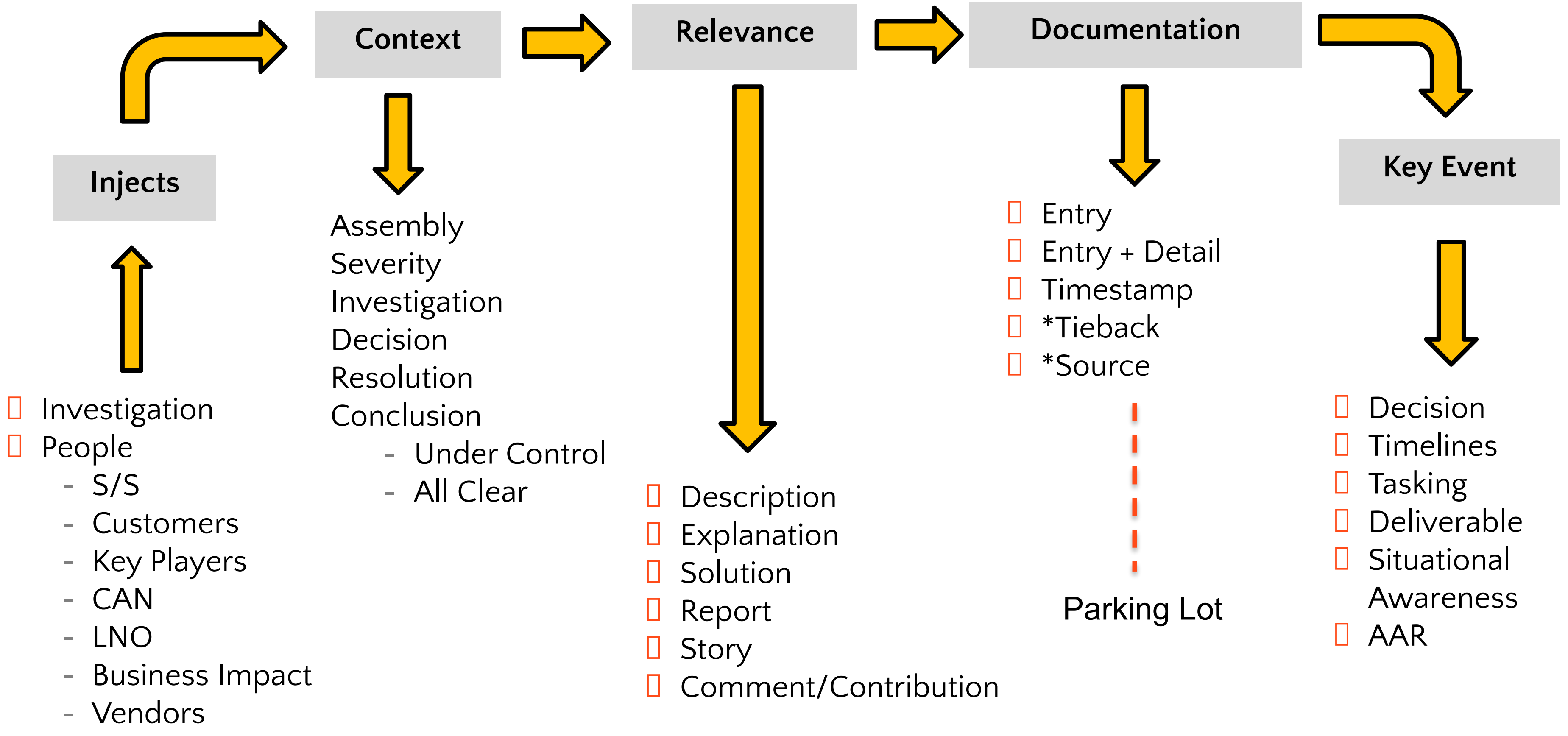
Questions
Data
Ideas
Clues
Statements
Needs
Actions
SOP

<u>Signs</u>
Countable
Objective
Observable by others
Described

<u>Symptoms</u>
Uncountable
Subjective
Not observable by others
Described

Tactical Documentation

Consider - Capture - Condense



Injects

- Investigation
- People
  - S/S
  - Customers
  - Key Players
  - CAN
  - LNO
  - Business Impact
  - Vendors

Context

Assembly
Severity
Investigation
Decision
Resolution
Conclusion

- Under Control
- All Clear

Relevance

- Description
- Explanation
- Solution
- Report
- Story
- Comment/Contribution

Documentation

- Entry
- Entry + Detail
- Timestamp
- *Tieback
- *Source

Parking Lot

Key Event

- Decision
- Timelines
- Tasking
- Deliverable
- Situational Awareness
- AAR

Tactical Documentation

People

- Identify each participant by name and function

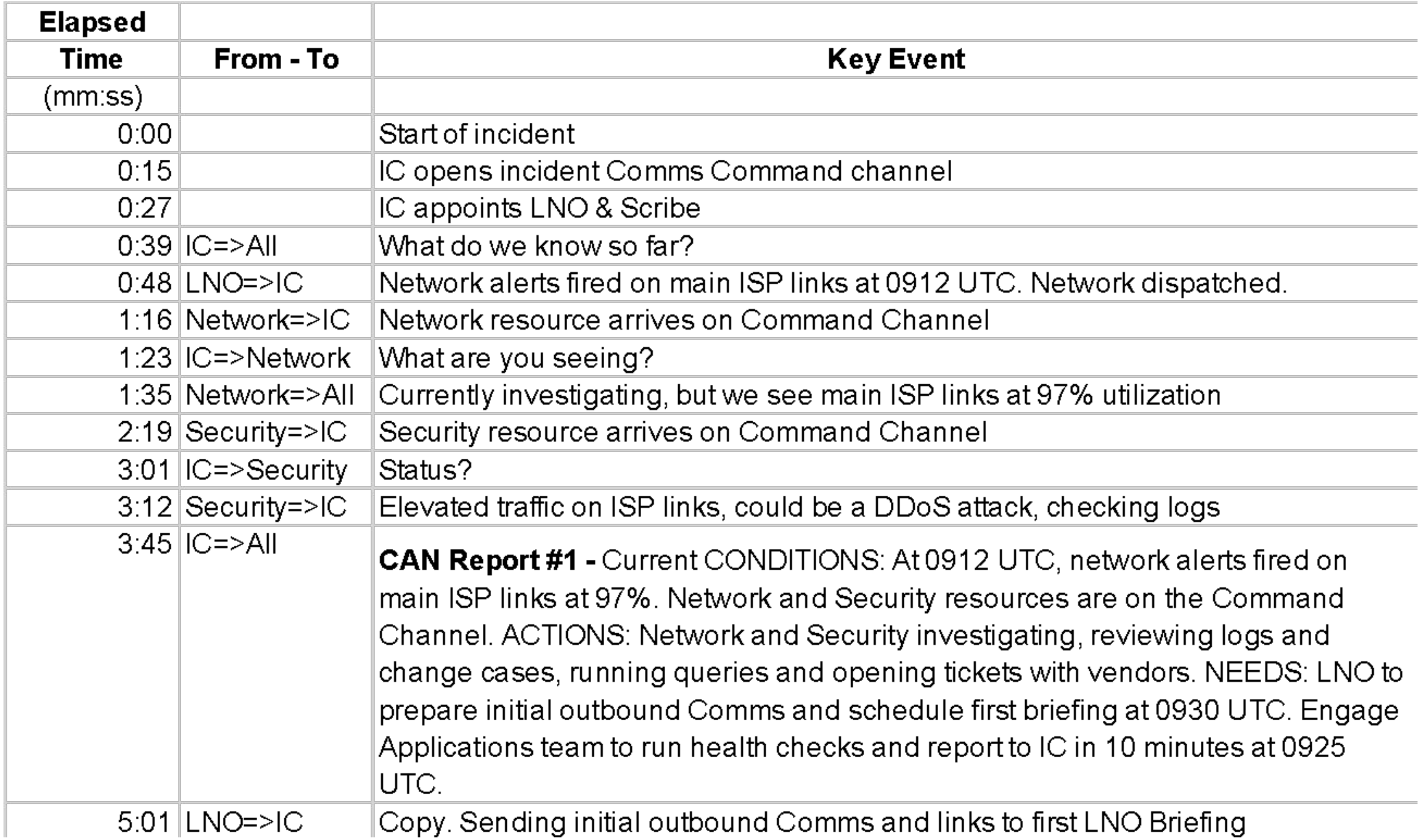
Conditions (Signs and Symptoms)

- Be specific and accurate
- Use precise numbers when known
- Write in bullet point format
- Don't capture technical jargon unless certain all will understand

Key Events

- Time: Start time, briefing times, elapsed time of the incident
- CAN Reports
- Briefing content and cadence
- Positive/negative state change
- Key decisions and logic
- Assigned tasks/work products
- Expected reactions to actions taken

Tactical Documentation



Elapsed		
Time	From - To	Key Event
(mm:ss)		
0:00		Start of incident
0:15		IC opens incident Comms Command channel
0:27		IC appoints LNO & Scribe
0:39	IC=>All	What do we know so far?
0:48	LNO=>IC	Network alerts fired on main ISP links at 0912 UTC. Network dispatched.
1:16	Network=>IC	Network resource arrives on Command Channel
1:23	IC=>Network	What are you seeing?
1:35	Network=>All	Currently investigating, but we see main ISP links at 97% utilization
2:19	Security=>IC	Security resource arrives on Command Channel
3:01	IC=>Security	Status?
3:12	Security=>IC	Elevated traffic on ISP links, could be a DDoS attack, checking logs
3:45	IC=>All	**CAN Report #1 -** Current CONDITIONS: At 0912 UTC, network alerts fired on main ISP links at 97%. Network and Security resources are on the Command Channel. ACTIONS: Network and Security investigating, reviewing logs and change cases, running queries and opening tickets with vendors. NEEDS: LNO to prepare initial outbound Comms and schedule first briefing at 0930 UTC. Engage Applications team to run health checks and report to IC in 10 minutes at 0925 UTC.
5:01	LNO=>IC	Copy. Sending initial outbound Comms and links to first LNO Briefing

OnSite
Incident Management Training

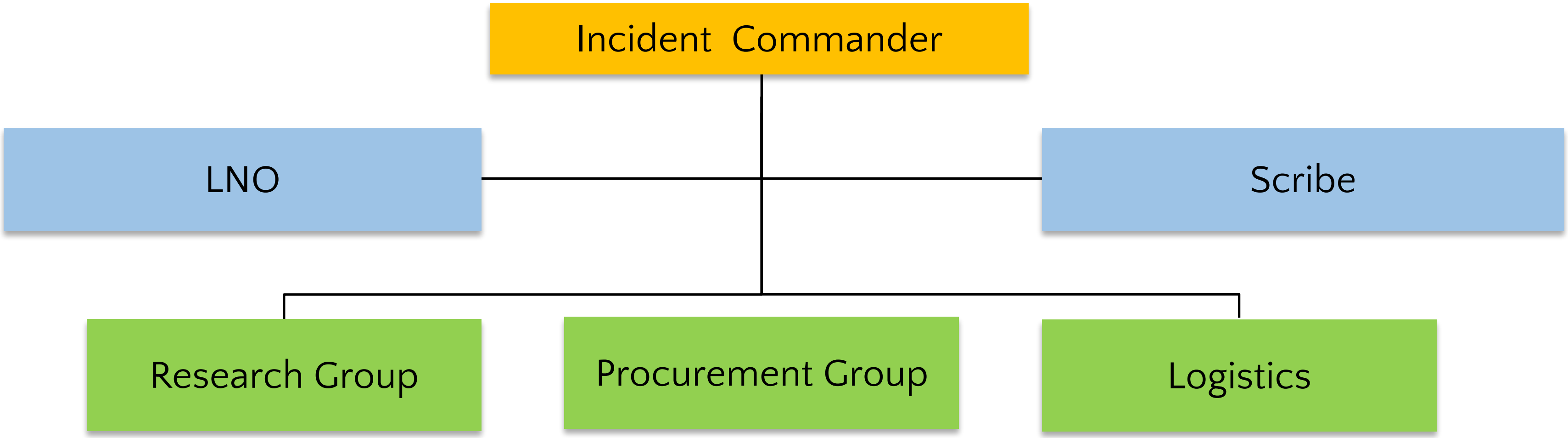
Lunch Break Exercise

© 2022 V1 Blackrock 3 Partners, Inc.

Lunch Exercise

- **Budget**
- **Considerations**
  - Dietary Restrictions
  - Restaurant Location
  - No fast food, filter organs, or pizza
- **Time**
- **Job Functions**
  - Incident Commander
  - LNO
  - Scribe
- **Communications**

Lunchtime Org Chart



5 minutes of preparation

Delegation!

Everyone is involved