Incident Reports and Logs

Incident reports and logs provide structured documentation of disruptive events, enabling root cause analysis and providing data to drive systemic improvements.

Incident Reports contain detailed information related to a specific disruptive event, including:

- Date/time/location of incident
- Description of what occurred
- Operational and business impacts
- Containment actions taken
- Estimated recovery time
- Indicators of likely root cause(s)
- Recommendations for prevention

Properly documenting incidents in a timely manner is critical for analysis. Reports should capture as much relevant detail as possible while the event is recent.

Incident Logs provide organized repositories of high-level incident information for tracking trends. Typical log contents:

- Incident ID
- Date/time
- Incident type/category
- Detection source
- Recovery time
- Root cause summary
- Process(es) impacted

The log provides vital data to perform analyses like:

- Identifying problem-prone processes
- Frequency and impact of different incident types
- Trends in recovery times
- Ranking common root causes

Detailed incident reports and centralized logs enable structured problem management approaches to reduce organizational risk. They are indispensable for continual improvement.