Incident after-action board report outline

*Working draft*

**Big picture**

- Reminder of crown jewels, biggest threats and risks, where this incident fits in our risk and detection profile
- Highlights of the incident and its impact (event summary, impacts including customers and third parties, regulatory, costs, current status)

**Details of the incident**

- Who was the attacker and what was their intent?
  - Data resources affected – ours or a 3rd party?
  - Were we the only/primary target, or who else was affected?
- Who reported it, how did we discover it?
  - Internal detection and reporting?
  - Third party detection?
- How did the attackers do it?
  - Was this a zero-day/new attack method?
  - How long were they in our systems?
  - Controls that were compromised?
  - Third parties/vendor compromise?
- What was our response and when?
  - Operational/technical, legal and compliance, communications?
  - Did we collaborate with others on the detection, investigation, response?

**Long-term impact and actions**

- Is this an ongoing issue? How much of a risk priority is it?
- Are there steps we can/are taking to minimize the long-term risk?
  - People, process, technology, cost