**Cybersecurity Templates**

**Incident Report Excel Model**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Incident Report Excel Model** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | IR‑DIR‑MOD‑[####] | **Owner:** | [Head of CSIRT / Security Operations] |
| **Approver:** | [CISO / Operations Governance Board] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Incident Report Excel Model 3](#_Toc207306673)

[Sheet: Data (supporting lists & mappings) — tblData 3](#_Toc207306674)

[A. Core Lists (single column each, start at row 2) 3](#_Toc207306675)

[B. SLA by Severity (two columns starting row 2) — named range SLA\_Days 3](#_Toc207306676)

[C. Impact Mapping (four columns) — named range Impact\_Map 4](#_Toc207306677)

[Sheet: Incident\_Register — tblIncidents 4](#_Toc207306678)

[Sheet: Case\_Details — tblDetails 5](#_Toc207306679)

[Sheet: Evidence\_Register — tblEvidence 6](#_Toc207306680)

[Sheet: Actions\_Recovery — tblActions 7](#_Toc207306681)

[Sheet: Comms\_Log — tblComms 7](#_Toc207306682)

[Sheet: Notifications — tblNotifs (optional) 7](#_Toc207306683)

[Build Notes & Good Practices 8](#_Toc207306684)

[Optional: Power Query / Automation Ideas 8](#_Toc207306685)

[Column Dictionary (for governance/data catalog) 8](#_Toc207306686)

[Minimal Example Rows (for testing) 9](#_Toc207306687)

# Incident Report Excel Model

A multi-sheet Excel workbook structure you can copy/paste directly into a new file. It’s designed for day-to-day IR logging **and** management reporting, with clean data validation, and is ready‑to‑build charts.

**Quick Start**

1. Create a new workbook and add the sheets below with the exact names.
2. Turn each table into an Excel Table (Ctrl/Cmd+T). Suggested Table names are in **bold**.
3. Add the data‑validation lists from **Data** to the other sheets.
4. Paste the sample formulas and adjust named ranges as needed.
5. Build the dashboard pivots from **Incident\_Register**, **Actions\_Recovery**, and **Comms\_Log**.

# Sheet: Data (supporting lists & mappings) — tblData

Put all drop-downs and mapping tables here. Keep one concept per block.

## A. Core Lists (single column each, start at row 2)

* **Incident\_Type**: Phishing, Malware, Ransomware, BEC, Data Breach, DoS/DDoS, Web App, Insider, Misconfiguration, Lost/Stolen Device, Supply Chain, Other
* **Source\_Vector**: Email, Web, External Media, Attrition, Impersonation, Supply Chain, Improper Usage, Loss/Theft, Other
* **Detection\_Source**: User Report, SOC Alert, MSSP, Third Party, Law Enforcement, Media
* **Status**: New, Triage, Containment, Eradication, Recovery, Monitoring, Resolved, Closed
* **Severity**: Low, Medium, High, Critical
* **Sensitivity**: Public, Internal, Confidential, Restricted
* **CIA\_Level** (0–3): 0, 1, 2, 3
* **Root\_Cause**: Human Error, Policy Gap, Control Failure, Vulnerability Exploit, Social Engineering, Misconfiguration, Third‑party, Unknown
* **Regulator** (optional): [list your regulators/obligations]

## B. SLA by Severity (two columns starting row 2) — named range SLA\_Days

* Severity | SLA\_Days (calendar)
* Low | 10
* Medium | 5
* High | 2
* Critical | 1

## C. Impact Mapping (four columns) — named range Impact\_Map

* Label | CIA\_Score | Business\_Impact | Score
* (CIA\_Score is 0–9 = C+I+A; Business\_Impact: Low=1, Med=2, High=3, Critical=4)
* Use this tiny map for consistent severity scoring.

Tip: Select each list block and create a Named Range matching the bold name (Formulas ▶︎ Name Manager). Use those names in validation and formulas.

# Sheet: Incident\_Register — tblIncidents

One row per incident. Keep the text fields short; push long narratives to **Case\_Details**.

**Columns (in order)**

1. **Incident\_ID** (text) – auto pattern INC-YYYY-#### (see formula below)
2. **Occurred\_At** (datetime)
3. **First\_Detected** (datetime)
4. **Reported\_By** (text)
5. **Detection\_Source** (DV: =Detection\_Source)
6. **Incident\_Type** (DV: =Incident\_Type)
7. **Source\_Vector** (DV: =Source\_Vector)
8. **Affected\_Asset\_ID** (text)
9. **Affected\_System** (text)
10. **Data\_Sensitivity** (DV: =Sensitivity)
11. **C\_Impact** (DV: =CIA\_Level)
12. **I\_Impact** (DV: =CIA\_Level)
13. **A\_Impact** (DV: =CIA\_Level)
14. **CIA\_Score** (calc) = C\_Impact + I\_Impact + A\_Impact
15. **Business\_Impact** (DV: Low, Medium, High, Critical)
16. **Initial\_Severity** (DV: =Severity)
17. **Calc\_Severity** (calc, optional — see formula)
18. **Owner** (text)
19. **Status** (DV: =Status)
20. **Summary** (short text)
21. **Time\_to\_Detect\_h** (calc)
22. **Time\_to\_Contain\_h** (calc)
23. **Time\_to\_Recover\_h** (calc)
24. **SLA\_Due** (date — from severity)
25. **Notifs\_Required** (Yes/No)
26. **Regulator** (DV: =Regulator)
27. **Report\_Due** (date)
28. **Reported\_On** (date)
29. **Root\_Cause** (DV: =Root\_Cause)
30. **Lessons\_Tag** (short text; for PIR linking)

**Sample formulas (enter once in row 2 of the Table; Excel will fill down):**

* **Incident\_ID**: ="INC-" & TEXT([@Occurred\_At],"yyyy") & "-" & TEXT(ROW()-1,"0000")
  + For robust IDs, consider Power Query or Office Script to assign sequence numbers.
* **CIA\_Score**: =[@C\_Impact]+[@I\_Impact]+[@A\_Impact]
* **Calc\_Severity** (example rule: max of CIA and Business impact):  
  =IF([@Business\_Impact]="Critical","Critical", IF([@CIA\_Score]>=7,"High", IF([@CIA\_Score]>=4,"Medium","Low")))
  + Or use =XLOOKUP([@Severity],Impact\_Map[Label],Impact\_Map[Score]) if you maintain a richer map.
* **Time\_to\_Detect\_h**: =IF([@First\_Detected]="",, ([@First\_Detected]-[@Occurred\_At])\*24)
* **Time\_to\_Contain\_h**: =IF([@Status]="",, ([@Containment\_Complete]-[@First\_Detected])\*24) *(add a hidden* ***Containment\_Complete*** *column if you track timestamps)*
* **Time\_to\_Recover\_h**: =IF([@Recovery\_Complete]="",,([@Recovery\_Complete]-[@First\_Detected])\*24) *(add* ***Recovery\_Complete*** *similarly)*
* **SLA\_Due**: =[@First\_Detected] + XLOOKUP([@Initial\_Severity],SLA\_Days[Severity],SLA\_Days[SLA\_Days])
* **Report\_Due**: =IF([@Notifs\_Required]<>"Yes","",[@First\_Detected]+1) *(example: 24h obligation — adjust to your regime)*

**Conditional Formatting (suggested)**

* If **Status** <> Closed and **SLA\_Due** < Today → highlight row.
* If **Notifs\_Required** = Yes and **Reported\_On** is blank → highlight cell.
* Heat‑scale on **Time\_to\_Recover\_h** for MTTR visuals.

# Sheet: Case\_Details — tblDetails

Extended narrative and investigation artifacts keyed by **Incident\_ID**.

**Columns**

* Incident\_ID (DV from tblIncidents[Incident\_ID])
* Long\_Description (free text)
* Hypothesis (free text)
* TTPs\_Observed (MITRE tags)
* Affected\_Accounts (text)
* Persistence\_Indicators (text)
* Lateral\_Movement (text)
* Data\_At\_Risk (text)
* Evidence\_Links (file paths/IR platform links)
* Containment\_Actions (free text)
* Eradication\_Actions (free text)
* Recovery\_Actions (free text)
* Validation\_Checks (free text)

Tip: Use **XLOOKUP** from a slicer cell holding the selected Incident\_ID to display summarised fields from **tblIncidents** in a header area for context.

# Sheet: Evidence\_Register — tblEvidence

Chain‑of‑custody style logging.

**Columns**

* Incident\_ID
* Item\_ID
* Description
* Qty/Type
* Serial\_or\_Hostname
* MAC
* IP
* Hash
* Collected\_By (name/title)
* Collected\_At (date/time & location)
* Storage\_Location
* Accessed\_By
* Accessed\_At
* Notes

**Validation & Protection**

* Lock **Hash**, **Collected\_By**, **Collected\_At** after entry (sheet protection) to preserve chain‑of‑custody.

# Sheet: Actions\_Recovery — tblActions

Track remediation and improvement tasks.

**Columns**

* Incident\_ID
* Action\_ID
* Category (Contain, Eradicate, Recover, Improve)
* Action
* Owner
* Status (Not started, In Progress, Blocked, Complete)
* Due\_Date
* Completed\_On
* Evidence\_Link
* PIR\_Tag (text)

**KPI helper columns** (optional)

* Days\_Open: =IF([@Completed\_On]="", TODAY()-[@Due\_Date], [@Completed\_On]-[@Due\_Date])
* On\_Time: =IF([@Completed\_On]="", "", IF([@Completed\_On] <= [@Due\_Date], "Yes", "No"))

# Sheet: Comms\_Log — tblComms

Keep a timeline of factual updates.

**Columns**

* Incident\_ID
* Entry\_DateTime
* Audience (Internal, Exec, Regulator, Customer, Public)
* Medium (Email, Call, Portal, Press)
* Summary
* Next\_Update\_Due
* Owner

# Sheet: Notifications — tblNotifs (optional)

Pre-stage reporting requirements.

**Columns**

* Incident\_ID
* Obligation (e.g., data breach law, sector regulator)
* Trigger (e.g., personal data exfil, outage > X hours)
* Deadline (hours)
* Due\_At (calc): =[@[First\_Detected]] + [@[Deadline]]/24
* Submitted\_At
* Reference

**Sheet: Dashboard (pivots & charts)**

Build visuals from the tables above. Suggested tiles:

* **Open Incidents by Severity** (clustered column)
* **MTTD / MTTR by Month** (line)
* **Top Incident Types (last 90 days)** (bar)
* **Incidents by Source Vector** (pie or bar)
* **Regulatory Notifications (YTD)** (card: count submitted / overdue)
* **Actions On‑Time Rate** (gauge or bar)

Add Slicers for Severity, Incident\_Type, Owner, Status, and a Timeline on Occurred\_At.

# Build Notes & Good Practices

* Use Excel **Tables** everywhere; avoid merged cells.
* Keep all lists and mappings in **Data** and refer via **named ranges**.
* Prefer **structured references** in formulas; they auto-fill and are pivot-friendly.
* Minimise free‑text: if you can make it a drop-down, do it.
* Lock the **Evidence\_Register** after entries; keep a copy of the workbook in a controlled location.
* For multi-team environments, consider SharePoint/OneDrive with versioning; for higher assurance, log evidence in a case‑management tool and link back using **Evidence\_Links**.

# Optional: Power Query / Automation Ideas

* Auto-generate **Incident\_ID** via a PQ step that adds an index per year.
* Create a refreshable **Calendar** table for time‑series metrics.
* Use Office Scripts/Power Automate to create regulator notice stubs when **Notifs\_Required** = Yes.

# Column Dictionary (for governance/data catalog)

* **Incident\_ID**: Unique key across all sheets.
* **Occurred\_At**/**First\_Detected**: UTC recommended; store local offset separately if needed.
* **CIA\_Score**: Sum of C/I/A impacts (0–9) for quick triage.
* **Calc\_Severity**: Derived from CIA and Business Impact for consistency.
* **Notifs\_Required**/**Report\_Due**/**Reported\_On**: Tracks statutory or contractual notifications.
* **PIR\_Tag/Lessons\_Tag**: Free tags to correlate with post-incident reviews.

# Minimal Example Rows (for testing)

Add one or two fake incidents to test pivots and dashboards (do **not** use real data in a template copy):

* INC-2025-0001, Phishing via Email, Internal data, CIA 1/1/0, Medium, Owner=Aisha, Status=Containment.
* INC-2025-0002, Ransomware, High sensitivity, CIA 3/3/3, Critical, Owner=SOC, Status=Recovery.