Automated Risk Register Orchestration Engine (ARROE)

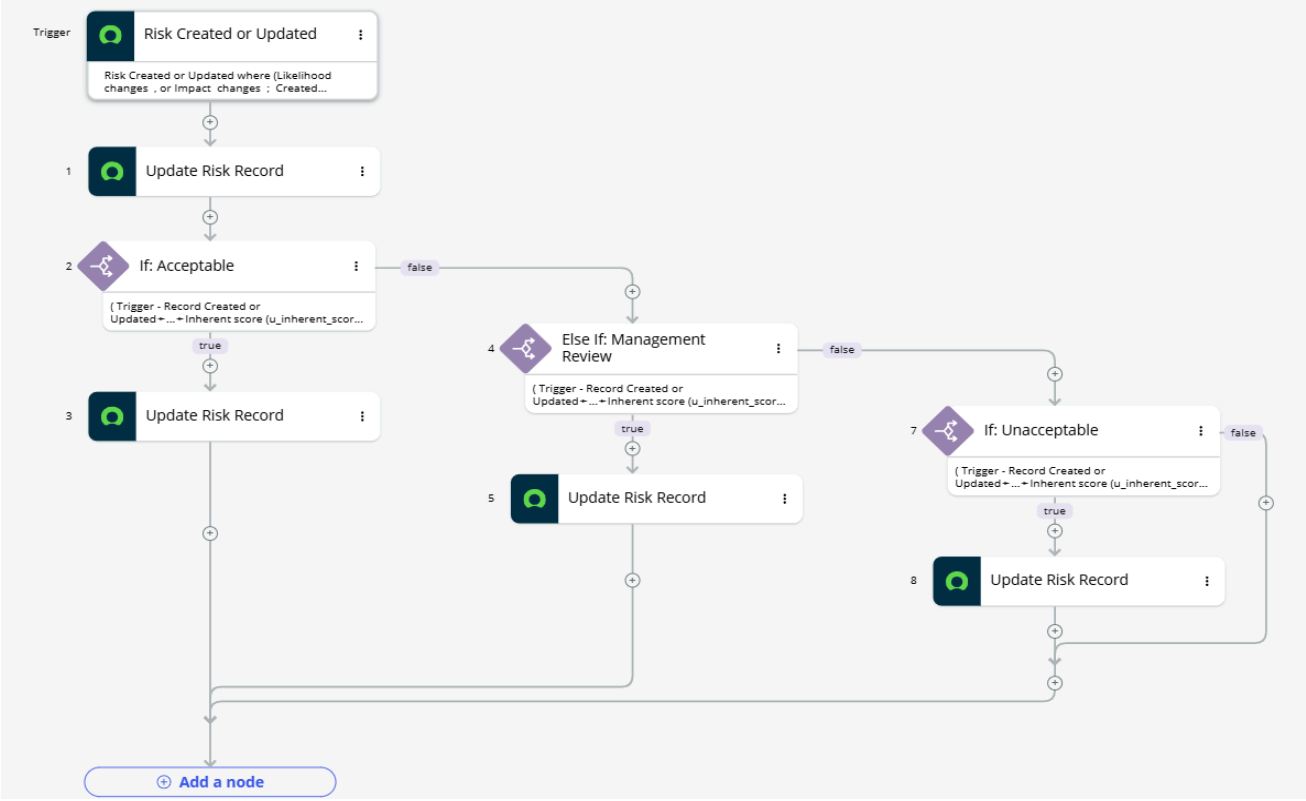
NimbusTech Inc.

Documented by : Om Satam

Description:

An enterprise-grade GRC Risk Register automation project built on ServiceNow. The system ingests risk data from an ISO 27001-aligned ISMS risk register (CSV import), automatically calculates Inherent Risk Scores based on Likelihood × Impact, and enforces predefined risk rating thresholds (Acceptable, Management Review, Must Treat). Each risk is auto-numbered with a globally unique ID for audit traceability and linked to Statement of Applicability (SoA) controls for compliance mapping. Flow Designer automation ensures consistent classification, duplicate prevention, and dynamic updates only when risk parameters change, reducing human error and streamlining governance workflows.

Architecture / Flow Summary



The automation is implemented in ServiceNow Flow Designer and follows a structured sequence to ensure risks are consistently evaluated and classified.

Workflow Steps:

1. **Trigger**
    - The flow is triggered whenever a Risk record is **created** or when the **Likelihood** or **Impact** values are updated.
    - This ensures Risk Rating is only recalculated when relevant inputs change.
2. **Calculate Inherent Score**
    - The system multiplies **Likelihood × Impact** to generate the **Inherent Score (u_inherent_score)**.
    - This forms the basis for objective, quantitative risk evaluation.
3. **Evaluate Thresholds (If / Else If / Else)**
    - The Inherent Score is passed through conditional logic:
        - **If ≤ 8** → Risk Rating = Acceptable.
        - **Else If 9–11** → Risk Rating = Management Review.
        - **Else (≥12)** → Risk Rating = Unacceptable – Must Treat.
    - Each branch includes guard conditions to prevent redundant updates.
4. **Update Risk Record**
    - The appropriate **Risk Rating (u_risk_rating)** is written back to the Risk record.
    - This creates a consistent, automated classification without manual intervention.

Value:
This flow eliminates human error, enforces ISMS methodology, and ensures that Risk Ratings remain dynamically aligned with the underlying data.

Import Process

The Risk Register is imported into ServiceNow using a controlled data pipeline to ensure accuracy and consistency:

1. **Source**
    - The source of truth is the CSV file exported from the ISMS Risk Register.
    - Each record includes the following fields:
        - **Name**
        - **Description**
        - **Likelihood**
        - **Impact**
        - **Treatment**
        - **Owner**
        - **Status**
        - **LinkedSoA**
2. **Staging**
    - Data is first loaded into the staging table **`u_risk_import`** using ServiceNow's Import Set mechanism.
    - This isolates raw imports from production data and allows validation before transformation.
3. **Transformation**
    - A **Transform Map** moves data from **`u_risk_import`** into the production table **`sn_risk_risk`.**
    - **Coalesce** is set on the **Name** field (case-insensitive).
        - If a matching Risk Name exists → the record is **updated**.
        - If no match exists → a new Risk is **inserted**.
4. **Safety & Integrity**
    - Coalesce prevents duplicate Risks from being created.
    - Any duplicate entries already present were cleaned up prior to enabling coalesce.
    - This ensures a **1:1 relationship** between Risk Register entries and records in ServiceNow.

Risk Rating Logic

Risk ratings are automatically calculated and assigned in ServiceNow based on the **Inherent Score (u_inherent_score)**. The thresholds are:

- **Acceptable** → u_inherent_score ≤ 8
- **Management Review** → 9 ≤ u_inherent_score ≤ 11
- **Unacceptable – Must Treat** → u_inherent_score ≥ 12

The field **Risk Rating (u_risk_rating)** is **auto-populated** via ServiceNow **Flow Designer logic** whenever a Risk record is created or updated. The logic evaluates the Inherent Score and dynamically updates the Risk Rating according to the thresholds above.

This automation ensures:

- Consistency in how Risk Ratings are assigned.
- Alignment with ISMS methodology.
- Reduced manual intervention and human error.

Risk Numbering

All risks are automatically assigned globally unique IDs using ServiceNow's **Business Rule** logic, ensuring auditability and traceability.

- **Prefix:** `NT-ISMS-RR`
- **Digits:** 4 (e.g., `NT-ISMS-RR0001`, `NT-ISMS-RR0002`)
- **Generation:** Sequentially generated at the time of record creation.

This automation guarantees that:

- Each risk is uniquely identifiable.
- Risk records can be reliably tracked across imports, updates, and audits.
- The numbering sequence aligns with ISMS documentation standards for NimbusTech Inc.

Security & Hardening Notes

To ensure the accuracy, reliability, and security of the Risk Register automation, the following hardening measures were implemented:

1. **Duplicate Prevention**
    - Transform Map configured with **Coalesce on Name** to prevent creation of duplicate risk records during CSV imports.
    - Any duplicates created during early testing were safely cleaned up.
2. **Flow Optimization**
    - Flow Designer logic includes guard conditions so that Risk Rating updates only occur when **Likelihood** or **Impact** values change, or when the record is first created.
    - This reduces unnecessary executions and ensures data integrity.
3. **Idempotent Updates**
    - Branch conditions check whether a Risk Rating is already set to the correct value before updating.
    - Prevents redundant writes and reduces audit log noise.
4. **Null/Blank Safety**
    - Logic ensures that Risk Rating is not calculated unless a valid **Inherent Score** exists.
    - This avoids misclassification of incomplete records.
5. **Auditability**
    - Auto-numbering of risks ensures globally unique IDs.
    - Flow executions are logged in ServiceNow for full traceability.

Final Deliverables

This project demonstrates a full lifecycle **Risk Register Automation** aligned with ISO 27001 methodology and implemented in ServiceNow GRC.

Deliverables:

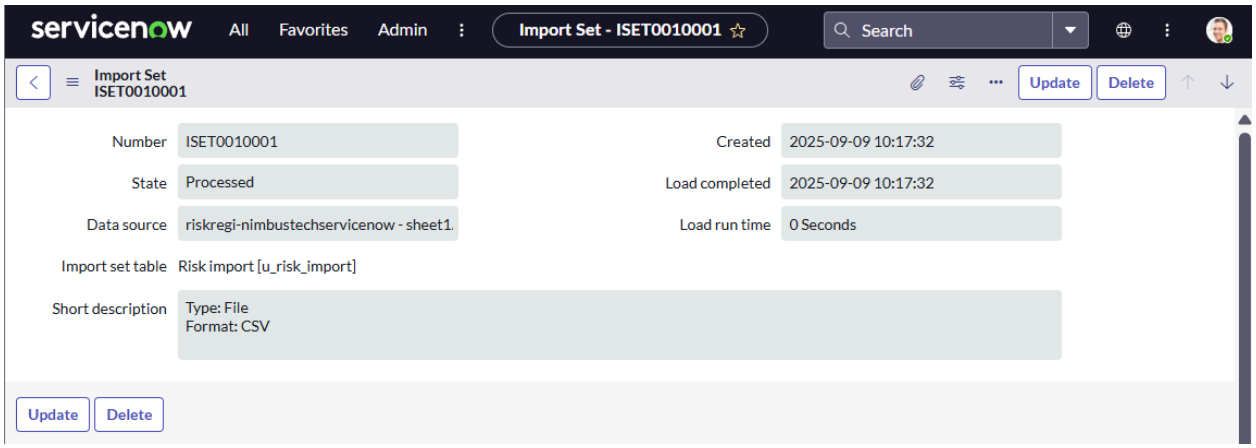
- **Risk Register Import Pipeline**
  - CSV-based ISMS Risk Register ingested into ServiceNow via staging + transform.
  - Duplicate prevention enforced with Coalesce on Name.
- **Custom Risk Fields**
  - Inherent Score (`u_inherent_score`), Risk Rating (`u_risk_rating`), Treatment (`u_treatment`), Status (`u_status`), LinkedSoA (`u_linkedsoa`).
- **Risk Rating Automation**
  - Flow Designer logic dynamically calculates Inherent Score and assigns Risk Ratings based on thresholds (Acceptable, Management Review, Must Treat).
- **Auto-numbering**
  - Business Rule logic generates globally unique IDs (`NT-ISMS-RR0001`, etc.) for full auditability.
- **Security & Hardening**
  - Guard conditions, null checks, and idempotent logic to ensure data integrity and prevent redundant updates.
- **Reporting & Traceability**
  - Risks linked with SoA controls.
  - Data structured for dashboards (Risks by Rating, Owner, Treatment).

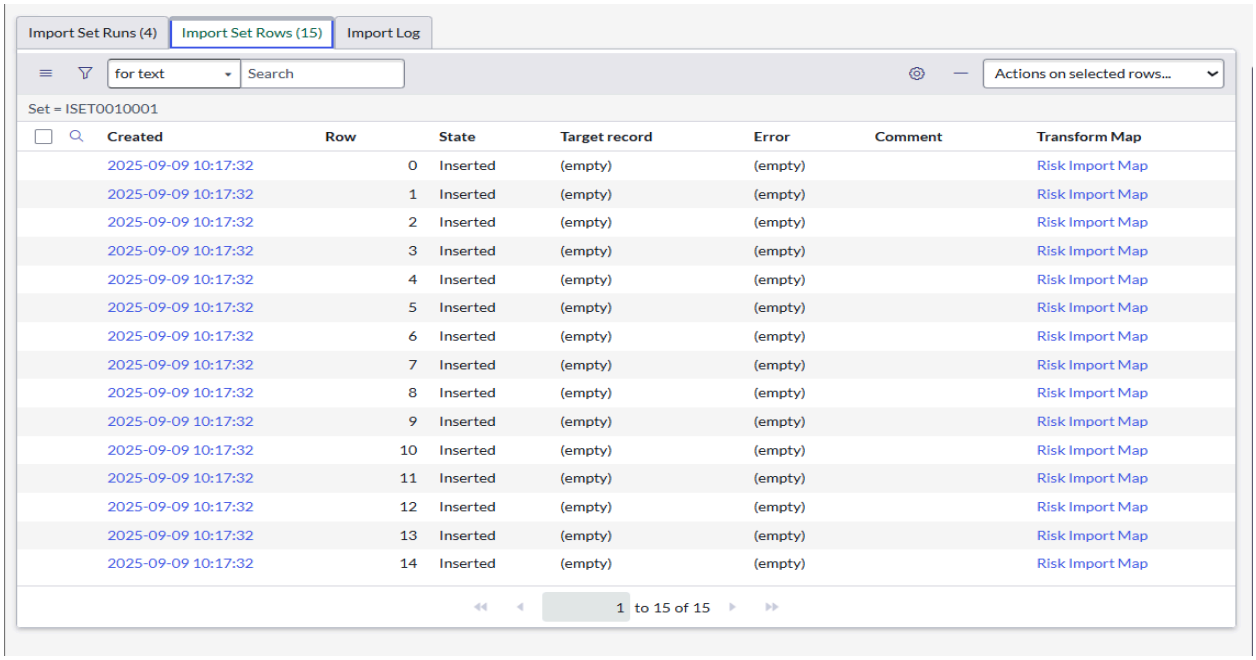
Screenshots

CSV

	A	B	C	D	E	F	G	H	I
1	Name	Descriptio	Likelihood	Impact	Treatment	Owner	Status	LinkedSoA	
2	Customer I	Unauthoriz	4	5	Mitigate	CISO	In Progress	A.5.1, A.5.2, A.8.34	
3	Cloud Stor	Data leaka	3	5	Mitigate	IT Manager	Open	A.5.23, A.8.9	
4	Employee I	Malware vi	4	4	Mitigate	HR Manag	In Progress	A.5.7, A.8.16	
5	SaaS Appli	Exploitatio	3	5	Mitigate	Dev Lead	Open	A.5.8, A.8.28	
6	Backup Sys	Ransomwa	3	5	Mitigate	IT Manager	In Progress	A.8.10	
7	Test Enviro	Leakage of	3	4	Mitigate	QA Lead	Planned	A.8.11	
8	Vendor Ser	Vendor mis	3	4	Transfer	Procureme	Open	A.8.30	
9	HR Record	Breach of e	3	4	Mitigate	HR Manag	Open	A.5.34	
10	Applicatior	Logs tampe	2	5	Mitigate	IT Security	In Progress	A.8.15, A.8.16	
11	Customer I	DDoS Attac	3	5	Mitigate	IT Manager	Planned	A.8.6, A.8.16	
12	Finance sy	Fraudulent	2	5	Mitigate	CFO	Open	A.5.2, A.8.15	
13	Compliance	Fines for m	2	4	Transfer	Compliance	Planned	A.5.5	
14	Email Acco	Account co	3	4	Mitigate	IT Security	Open	A.5.7, A.8.16	
15	DevOps Pi	Code leake	3	4	Transfer	Dev Lead	Open	A.8.28, A.8.30	
16	Cloud Infra	Capacity o	2	5	Mitigate	IT Manager	In Progress	A.8.6, A.8.16	
17									

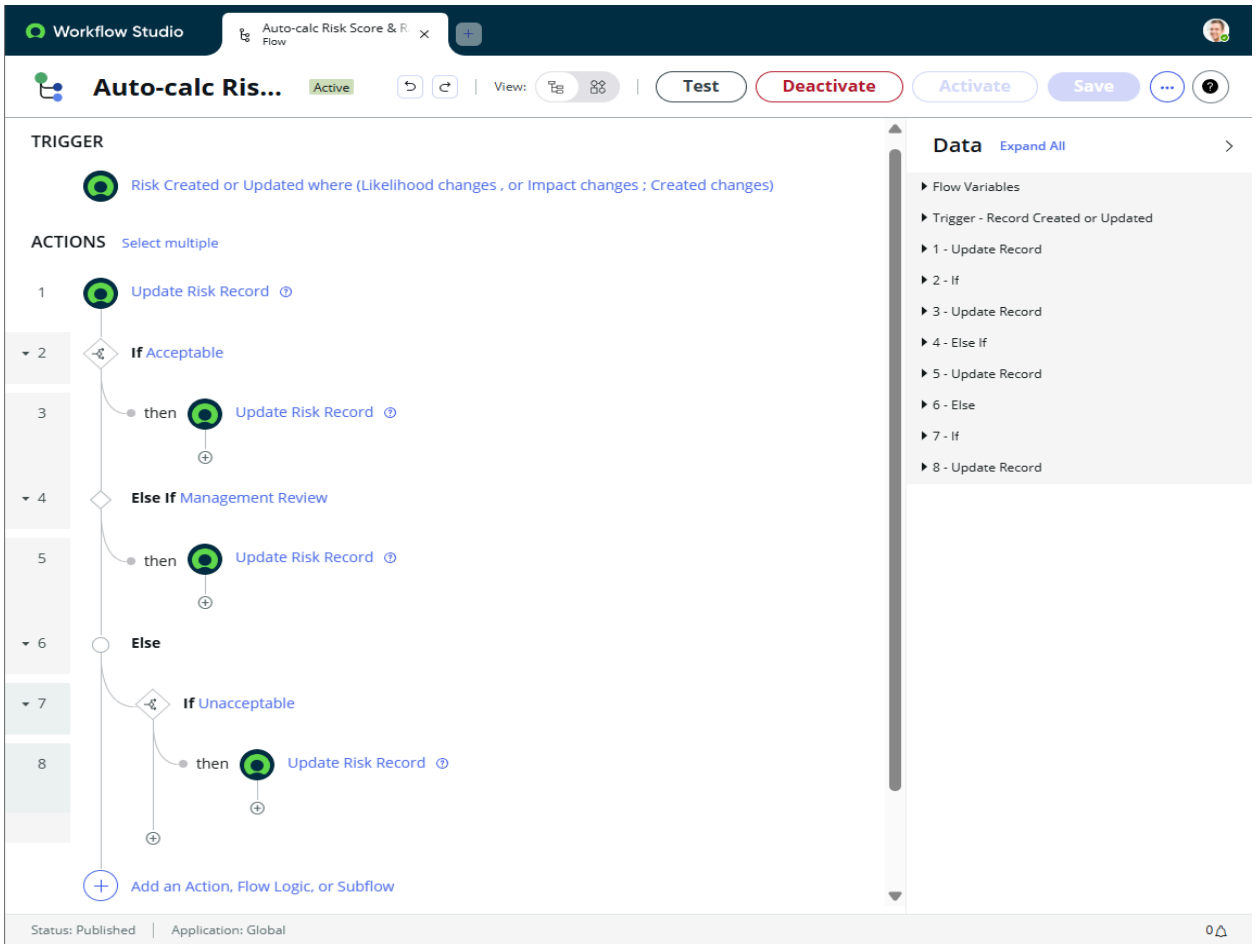
Imported Sets



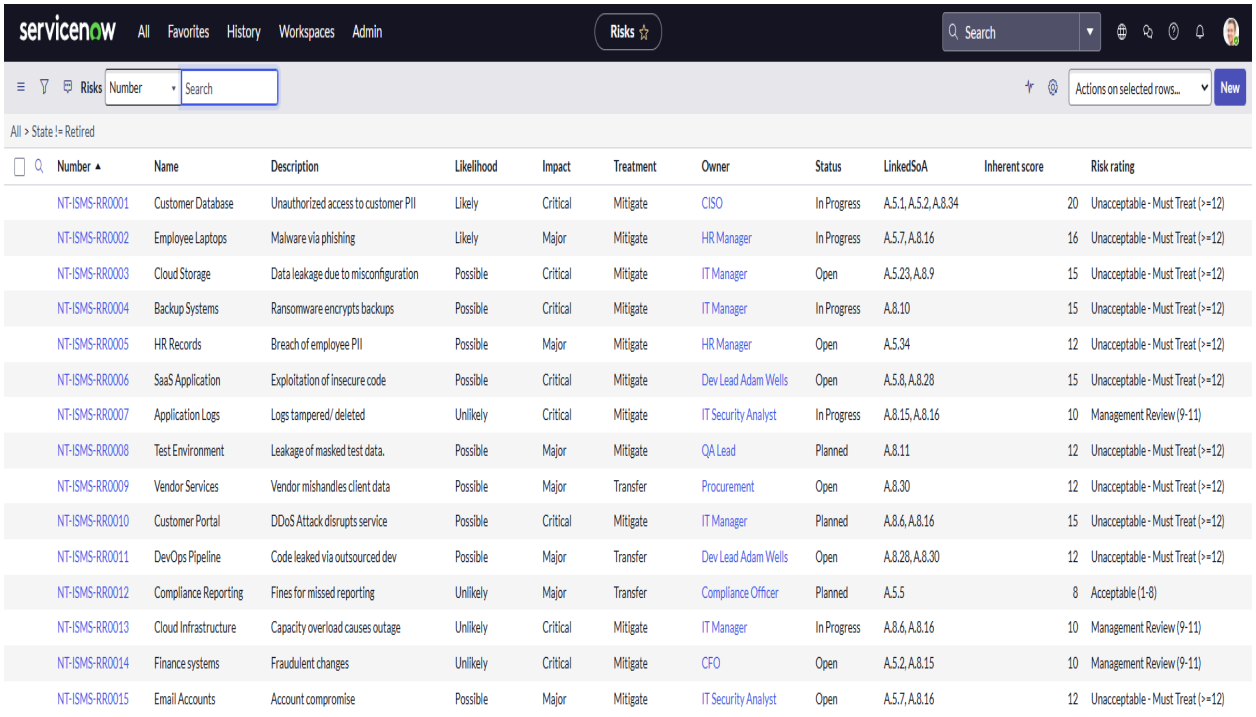


Created	Row	State	Target record	Error	Comment	Transform Map
2025-09-09 10:17:32	0	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	1	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	2	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	3	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	4	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	5	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	6	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	7	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	8	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	9	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	10	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	11	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	12	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	13	Inserted	(empty)	(empty)		Risk Import Map
2025-09-09 10:17:32	14	Inserted	(empty)	(empty)		Risk Import Map

Flow Designer Automation



Risk Register



Number	Name	Description	Likelihood	Impact	Treatment	Owner	Status	LinkedSoA	Inherent score	Risk rating
NT-ISMS-RR0001	Customer Database	Unauthorized access to customer PII	Likely	Critical	Mitigate	CISO	In Progress	A.5.1, A.5.2, A.8.34	20	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0002	Employee Laptops	Malware via phishing	Likely	Major	Mitigate	HR Manager	In Progress	A.5.7, A.8.16	16	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0003	Cloud Storage	Data leakage due to misconfiguration	Possible	Critical	Mitigate	IT Manager	Open	A.5.23, A.8.9	15	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0004	Backup Systems	Ransomware encrypts backups	Possible	Critical	Mitigate	IT Manager	In Progress	A.8.10	15	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0005	HR Records	Breach of employee PII	Possible	Major	Mitigate	HR Manager	Open	A.5.34	12	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0006	SaaS Application	Exploitation of insecure code	Possible	Critical	Mitigate	Dev Lead Adam Wells	Open	A.5.8, A.8.28	15	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0007	Application Logs	Logs tampered/ deleted	Unlikely	Critical	Mitigate	IT Security Analyst	In Progress	A.8.15, A.8.16	10	Management Review (9-11)
NT-ISMS-RR0008	Test Environment	Leakage of masked test data.	Possible	Major	Mitigate	QA Lead	Planned	A.8.11	12	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0009	Vendor Services	Vendor mishandles client data	Possible	Major	Transfer	Procurement	Open	A.8.30	12	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0010	Customer Portal	DDoS Attack disrupts service	Possible	Critical	Mitigate	IT Manager	Planned	A.8.6, A.8.16	15	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0011	DevOps Pipeline	Code leaked via outsourced dev	Possible	Major	Transfer	Dev Lead Adam Wells	Open	A.8.28, A.8.30	12	Unacceptable - Must Treat (>=12)
NT-ISMS-RR0012	Compliance Reporting	Fines for missed reporting	Unlikely	Major	Transfer	Compliance Officer	Planned	A.5.5	8	Acceptable (1-8)
NT-ISMS-RR0013	Cloud Infrastructure	Capacity overload causes outage	Unlikely	Critical	Mitigate	IT Manager	In Progress	A.8.6, A.8.16	10	Management Review (9-11)
NT-ISMS-RR0014	Finance systems	Fraudulent changes	Unlikely	Critical	Mitigate	CFO	Open	A.5.2, A.8.15	10	Management Review (9-11)
NT-ISMS-RR0015	Email Accounts	Account compromise	Possible	Major	Mitigate	IT Security Analyst	Open	A.5.7, A.8.16	12	Unacceptable - Must Treat (>=12)

Individual Risk Record eg. NT-ISMS-RR0001