Cheat Sheet QLRR

NT207 - CHEAT SHEET ÔN THI MANG VÀO PHÒNG THI

---

1. KHÁI NIỆM CƠ BẢN (ISO 31000:2018 + ISO 27000)

Khái niệm	Định nghĩa/Từ khóa chính
Rủi ro (Risk)	The effect of uncertainty on objectives (Tác động của sự không chắc chắn đến mục tiêu)
Sự kiện (Event)	Occurrence or change of a particular set of circumstances (Việc xảy ra hoặc thay đổi tình huống cụ thể)
Sự cố (Incident)	An event that has caused damage or loss (Một sự kiện đã gây thiệt hại hoặc tổn thất – rủi ro đã xảy ra)
Mối đe dọa (Threat)	Potential cause of an unwanted incident (Nguyên nhân tiềm ẩn gây sự cố không mong muốn)
Điểm yếu (Vulnerability)	Weakness that can be exploited by a threat (Yếu điểm có thể bị khai thác)
Khả năng xảy ra (Likelihood)	Chance of something happening (Cơ hội điều gì đó xảy ra)
Hệ quả (Consequence)	Outcome of an event affecting objectives (Kết quả của sự kiện ảnh hưởng đến mục tiêu)
Biện pháp kiểm soát (Control)	Measure that is modifying risk (Biện pháp điều chỉnh rủi ro)
Khẩu vị rủi ro (Appetite)	Amount and type of risk an organization is willing to pursue or retain (Mức rủi ro tổ chức sẵn sàng chấp nhận)
Rủi ro còn lại (Residual risk)	Risk remaining after risk treatment (Rủi ro còn lại sau khi xử lý)

2. MA TRẬN RỦI RO

Hậu quả \ Khả năng	Rất thấp	Thấp	TBình	Cao	Rất cao
Rất nghiêm trọng	Trung bình	Cao	Rất cao	Rất cao	Không chấp nhận
Nghiêm trọng	Thấp	TBình	Cao	Rất cao	Không chấp nhận
Trung bình	Thấp	TBình	TBình	Cao	Rất cao

Hậu quả \ Khả năng	Rất thấp	Thấp	TBình	Cao	Rất cao
Thấp	Chấp nhận	Thấp	TBình	TBình	Cao

3. 8 NGUYÊN TẮC QLRR (ISO 31000)

1. **Tích hợp**: gắn vào mọi hoạt động
2. **Có cấu trúc và toàn diện**
3. **Tùy chỉnh**
4. **Tham gia đầy đủ**
5. **Tính động**
6. **Thông tin tốt nhất có sẵn**
7. **Yếu tố con người và văn hóa**
8. **Cải tiến liên tục (PDCA)**

---

4. QUY TRÌNH QLRR (11 BƯỚC)

1. Lập kế hoạch
2. Nhận diện rủi ro (Risk Identification)
3. Phân tích rủi ro (Risk Analysis)
4. Đánh giá rủi ro (Risk Evaluation)
5. Xử lý rủi ro (Risk Treatment)
6. Kế hoạch xử lý rủi ro
7. Phê duyệt hồ sơ QLRR
8. Báo cáo kết quả
9. Theo dõi, đánh giá lại
10. Cải tiến, lưu hồ sơ
11. Lưu trữ, báo cáo định kỳ

---

5. MAPPING TÌNH HUỐNG → ISO 27001 (PHỤ LỤC A)

Tình huống	ISO 27001 Nhóm
Không có backup	A.12.3.1 (Backup data)
Không mã hóa email	A.13.2.3 (Electronic messaging)
Dùng Telnet	A.13.1.1 (Network control)

Tình huống	ISO 27001 Nhóm
Không đào tạo nhân viên	A.7.2.2
Không kiểm soát truy cập	A.9.1.1 (Access control policy)
Không có NDA với nhà cung cấp	A.15.1.1
Không có xử lý sự cố	A.16.1.1–16.1.7
Thiết bị phòng server đặt nơi dễ ngập	A.11.2.2
Phần mềm không có bản quyền	A.18.1.2

---

6. PHÂN BIỆT DỄ NHẦM

So sánh	Risk	Threat	Vulnerability
Tính chất	Dự đoán, tiềm ẩn	Cụ thể, thấy được	Cụ thể, yếu điểm
Yếu tố	Event + Likelihood + Consequence	Source gây ra Event	Có thể bị khai thác

📌 **Threat** khai thác điểm yếu **(vulnerability)** để tạo rủi ro **(Risk)**

Term	KPI	KRI
Câu hỏi	How well?	How risky?
Chức năng	Đo hiệu suất	Đo rủi ro
Gốc dữ liệu	Hiện tại/quá khứ	Dự báo tương lai

---

7. FMEA - CÔNG THỨC VÀ BẢNG

- RPN = Severity × Occurrence × Detectability
- Nếu RPN > ngưỡng → lập kế hoạch hành động 5W1H

Thành phần	Ý nghĩa	Thang điểm
Severity (Sev)	Mức độ nghiêm trọng	1–5 / 1–10
Occurrence (Occ)	Khả năng xảy ra	1–5 / 1–10
Detectability (Det)	Khả năng phát hiện	1–5 / 1–10

8. BCP – CHỈ SỐ PHỤC HỒI

Viết tắt	Ý nghĩa
RTO	Recovery Time Objective – thời gian hệ thống phải phục hồi tạm thời
RPO	Recovery Point Objective – thời gian dữ liệu có thể mất
WRT	Work Recovery Time – thời gian khôi phục hoàn toàn
MTD	Maximum Tolerable Downtime – Tổng thời gian ngừng tối đa = RTO + WRT

9. CÁC PHƯƠNG ÁN XỬ LÝ RỦI RO

Phương án	Mô tả
Chấp nhận (Accept)	Rủi ro nhỏ, không đáng xử lý
Giảm nhẹ (Mitigate)	Giảm xác suất hoặc tác động
Tránh né (Avoid)	Không làm hoạt động đó nữa
Chuyển giao (Transfer)	Bảo hiểm, thuê ngoài

Phương án	Khi nào dùng	Ví dụ
Chấp nhận	Rủi ro thấp, chấp nhận được	Mất điện 5p
Giảm nhẹ	Rủi ro cao, có thể giảm được	Cài phần mềm diệt virus
Tránh né	Rủi ro quá cao → bỏ luôn	Không triển khai dịch vụ
Chuyển giao	Đưa cho bên thứ 3	Mua bảo hiểm, thuê ngoài

10. KRI TIÊU BIỂU (Ví dụ)

Nhóm	KRI
Người	% nhân viên chưa đào tạo ATTT < 10%, % nhân viên nghỉ việc > 5%
Quy trình	Sự cố trùng lặp trong tháng = 0, thời gian khắc phục < 60p
Công nghệ	% uptime hệ thống > 99.72%, số cảnh báo phần mềm < 2/tháng

> **MẸO TRA CỨU NHANH**: Gắn bookmark hoặc dán giấy màu theo các phần: Thuật ngữ – Ma trận – ISO Mapping – PDCA – FMEA – BCP – KRI