Part 1 – Risk Exposure (RE) Calculations

1. RE Value for Each Non-Blank Entry (8 pts)

- For Root Cause 1 and Threat 1:
  P(E) = 0.20, L(E) = 25 → RE = 0.20 × 25 = **5.00**

- For Root Cause 1 and Threat 2:
  P(E) = 0.30, L(E) = 10 → RE = 0.30 × 10 = **3.00**

- For Root Cause 2 and Threat 1:
  P(E) = 0.30, L(E) = 15 → RE = 0.30 × 15 = **4.50**

- For Root Cause 3 and Threat 3:
  P(E) = 0.20, L(E) = 45 → RE = 0.20 × 45 = **9.00**

2. Total Risk Exposure for Each Root Cause (3 pts)

- Root Cause 1 total RE:
  5.00 (from Threat 1) + 3.00 (from Threat 2) = **8.00**

- Root Cause 2 total RE:
  4.50 (from Threat 1) = **4.50**

- Root Cause 3 total RE:
  9.00 (from Threat 3) = **9.00**

3. Total Risk Exposure for Each Threat (3 pts)

- Threat 1 total RE:
  5.00 (from RC1) + 4.50 (from RC2) = **9.50**

- Threat 2 total RE:
  3.00 (from RC1) = **3.00**

- Threat 3 total RE:
  4.50 (from RC3) = **9.00**

Conclusion of part 1:

- **Most Risky Root Cause / Threat Combo:**
  The **Root Cause 3 and Threat 3** pairing has the highest **individual RE of 9.00**. This suggests that "Inadequate resources to complete" is particularly dangerous in the context of Threat 3, likely due to high potential loss if exploited.

- **Root Cause with Highest Overall Risk:**
  Despite Root Cause 3 affecting only one threat, its RE of **9.00** makes it the most critical vulnerability to address. This highlights how a single, severe weakness can outweigh several lower-risk ones.

- **Threat with Highest Overall RE:**
  Threat 1, influenced by multiple root causes (1 and 2), accumulates the **highest RE of 9.50**, making it the most overall dangerous threat in the scenario. It's a priority for mitigation because it's broadly exposed to multiple vulnerabilities.

Part 2:

4. Using Table 2 – Risk Mitigation Evaluation

a) Is it worth enacting the Risk Mitigation action "Add Resources" to address Root Cause 2?

- From Table 1: Root Cause 2 affects Threat 1 with:
  - P(E) = 30%
  - L(E) = 15
  - Original RE = $0.30 \times 15 = 4.5$
- Table 2: "Add Resources" reduces P(E) by 10% and costs 5
- New P(E) = 30% - 10% = 20%
- New RE = $0.20 \times 15 = 3.0$
- Risk Reduction = 4.5 - 3.0 = 1.5

Answer: No, because the cost (5) outweighs the benefit (risk reduction of only 1.5)

b) Is it worth enacting the Risk Mitigation action "Add Resources" to address Root Cause 3?

- From Table 1: Root Cause 3 affects Threat 3 with:
    - P(E) = 20%
    - L(E) = 45
    - Original RE = 0.20 × 45 = 9.0
- Table 2: "Add Resources" reduces P(E) by 10%, cost = 5
- New P(E) = 20% - 10% = 10%
- New RE = 0.10 × 45 = 4.5
- Risk Reduction = 9.0 - 4.5 = 4.5

Answer: No, because the cost (5) outweighs the benefit (4.5)

c) Is it worth enacting the Risk Mitigation action "Prototype" to address Root Cause 1?

- From Table 1: Root Cause 1 affects Threat 1 and Threat 2
    - Threat 1: P(E) = 20%, L(E) = 25 → RE1 = 5.0
    - Threat 2: P(E) = 30%, L(E) = 10 → RE2 = 3.0
- Total RE = 5.0 + 3.0 = 8.0
- Table 2: "Prototype" reduces P(E) by 10% for Root Cause 1, cost = 3
- New P(E) for Threat 1 = 10% → RE1 = 0.10 × 25 = 2.5
- New P(E) for Threat 2 = 20% → RE2 = 0.20 × 10 = 2.0
- New Total RE = 2.5 + 2.0 = 4.5
- Risk Reduction = 8.0 - 4.5 = 3.5

Answer: Yes, because the cost (3) is less than the risk reduction (3.5)

d) Is it worth enacting the Risk Mitigation action "Add Resources" given the combined impact on Root Causes 2 and 3?

- Combined original RE:
    - RC2, Threat 1: 0.30 × 15 = 4.5
    - RC3, Threat 3: 0.20 × 45 = 9.0
    - Total = **13.5**
- After mitigation:
    - RC2: P(E) = 20% → 0.20 × 15 = 3.0
    - RC3: P(E) = 10% → 0.10 × 45 = 4.5
    - Total = **7.5**
- **Risk Reduction = 13.5 - 7.5 = 6.0**, Cost = **5**

Answer: Yes, the combined benefit (6.0) exceeds the cost (5)

5. Using Table 3, compute whether a contingency plan is worthwhile for that Root Cause (across the entire project)

a) **Contingency Action 1 – Litigation**

Cost: 15

Recovery: 50% for Threat 1

Calculate **Total Loss (L)** for Threat 1 across both root causes:

- RC1 Loss = 25
- RC2 Loss = 15
- **Total Loss = 25 + 15 = 40**

Recovered Value = 50% of 40 = 0.50 × 40 = 20
Compare to Cost (15): 20 > 15
Yes, this contingency plan is worthwhile for Threat 1.

Threat 2: Affected by One Root Cause

- RC1 only: 30% | 10
- **Contingency Action 2 – Purchase Insurance**
    - Cost: 12
    - Recovery: 60%

Recovered Value = 0.60 × 10 = 6
Compare to Cost (12): 6 < 12
No, not worthwhile

Part 3: Final Combined Mitigation and Contingency Planning Strategy

Based on the results from Parts 1 and 2, the most effective approach is to implement a targeted combination of mitigation and contingency strategies that deliver significant risk reduction at a reasonable cost.

Mitigation Strategy:

The "Prototype" action for Root Cause 1 is cost-effective and should be implemented. It reduces the total Risk Exposure (RE) for Threats 1 and 2 from 8.0 to 4.5, resulting in a risk reduction of 3.5 for a cost of only 3.

Individually, applying "Add Resources" to Root Cause 2 or Root Cause 3 was not cost-effective. However, applying "Add Resources" to both RC2 and RC3 together results in a combined RE reduction of 6.0 (from 13.5 to 7.5) for a cost of 5, which makes it worth implementing.

Contingency Strategy:

The "Deploy Software Patch" contingency for Threat 3 is highly recommended. It recovers 70% of the 45-unit loss (i.e., 31.5) at a cost of just 10, which is clearly cost-effective.

The "Litigation" contingency for Threat 1 does provide a recovery of 20, but at a cost of 15. Since the Prototype mitigation already reduces risk significantly for Threat 1, the added cost of litigation is not justified.

The "Purchase Insurance" contingency for Threat 2 is not recommended. It only recovers 6 units of value for a cost of 12, making it ineffective.

Final Recommendation:

- Implement **Prototype** for RC1
- Implement **Add Resources** for **both RC2 and RC3 combined**
- Implement **Deploy Software Patch** for **Threat 3**
- Do **not** implement Litigation or Insurance

This final plan minimizes overall risk while avoiding unnecessary cost. It strategically combines mitigation where risk can be prevented and contingency where the impact remains high even after mitigation. This provides the organization with an efficient and cost-conscious security strategy.