Residual Risk Calculation Detailed Example

The Scenario

We have a Data Breach Risk that we need to assess:

Inherent Risk (before any controls):

- Impact: 4 (catastrophic damage if it occurs)
- Likelihood: 4 (very likely to occur)
- Inherent Risk Score: 4 × 4 = 16 (Critical level)

We've implemented 4 security controls to mitigate this risk. Now we need to calculate the Residual Risk (what's left after controls are applied).

The Four Controls

Control	Type	Current Effectiveness
Firewall	Preventive	90%
IDS (Intrusion Detection System)	Detective	85%
Encryption	Technical	100%
Access Control	Technical	50%

Why these effectiveness levels?

- Firewall (90%): Has one overdue maintenance task, slightly reducing its effectiveness
- IDS (85%): Operating normally with no issues
- Encryption (100%): Perfect health, fully operational
- Access Control (50%): Has a medium-severity security incident, significantly degrading its effectiveness

Step 1: Understanding Control Types and Their Effects
Different types of controls affect different aspects of risk:
Controls that reduce Likelihood (prevent the event from happening):

- Preventive controls: Stop threats before they occur (e.g., Firewall blocks attacks)
- Organizational controls: Policies and procedures that prevent incidents
- Physical controls: Physical barriers (locks, security guards)
- Technical controls: Technology-based prevention AND detection

Controls that reduce Impact (minimize damage when events occur):

- Detective controls: Identify incidents quickly (e.g., IDS alerts on breaches)
- Corrective controls: Restore systems after incidents (e.g., backups)
- Technical controls: Can also minimize damage through automation

Note: Technical controls are dual-purpose—they affect both Likelihood and Impact.

Step 2: Classifying Our Controls
Based on their types:
Likelihood Controls (prevent the breach):
1. Firewall (90%) - Preventive type
2. Encryption (100%) - Technical type
3. Access Control (50%) - Technical type

Impact Controls (minimize damage if breach occurs):
1. IDS (85%) - Detective type
2. Encryption (100%) - Technical type
3. Access Control (50%) - Technical type

Notice that Encryption and Access Control appear in both lists because they're Technical controls.

Part A: Calculating Likelihood Reduction

Step 1: Convert Percentages to Decimals
We express effectiveness as decimals for calculations:

- Firewall: 90% = 0.9
- Encryption: 100% = 1.0
- Access Control: 50% = 0.5

Total: 0.9 + 1.0 + 0.5 = 2.4

Step 2: Calculate Average Effectiveness
We have 3 controls affecting likelihood.
Average Effectiveness = 2.4 ÷ 3 = 0.8 (or 80%)

Why use average? This represents the typical quality of our controls. If we just added them up (240%), it would incorrectly suggest we've eliminated more than 100% of the risk, which is impossible. The average also makes degradation visible—one poorly performing control brings down the overall average.

Step 3: Apply the Control Count Multiplier
Having multiple controls provides layered defense. Each additional control catches threats that others might miss. However, there are diminishing returns because controls start to overlap.
The multiplier formula accounts for this:
Multiplier = 1.0 + (0.5 × number of extra controls)
We have 3 controls, so:

- First control: counted as 1.0 (full value)
- Extra controls: 3 - 1 = 2 extra controls
- Bonus from extra controls: 0.5 × 2 = 1.0
- Total Multiplier: 1.0 + 1.0 = 2.0

What this means:

Number of Controls	Multiplier	Meaning
1 control	1.0	First control at full value
2 controls	1.5	Second control adds 50% bonus
3 controls	2.0	Third control adds another 50% bonus
4 controls	2.5 (capped at 2.0)	Fourth control adds 50% but hits cap

The multiplier is capped at 2.0 because beyond a certain point, additional controls provide minimal extra benefit due to overlap.

Step 4: Calculate the Reduction Factor
We combine average effectiveness with the multiplier:
Reduction Factor = Average Effectiveness × Multiplier
Reduction Factor = 0.8 × 2.0 = 1.6
This suggests our controls could theoretically reduce likelihood by 160%, but that's impossible.

Step 5: Apply the 90% Maximum Reduction Cap
No control set is perfect. There are always:

- Unknown vulnerabilities
- Black swan events
- Human errors
- Zero-day exploits

Therefore, we cap the maximum reduction at 90%:
Capped Reduction Factor = minimum of (1.6, 0.90) = 0.90
This means our controls can reduce likelihood by at most 90%.

Step 6: Apply the Dampening Factor
Even well-designed controls don't work perfectly in the real world due to:

- Implementation gaps
- Configuration drift over time
- User errors
- Integration issues
- Incomplete coverage

We apply a dampening factor of 0.85 (85%) to account for this reality:
Actual Reduction = 0.90 × 0.85 = 0.765 (76.5%)
This means our controls will actually reduce likelihood by 76.5% in practice.

Step 7: Calculate New Likelihood
Starting from our inherent likelihood of 4:
Remaining Likelihood = 100% - 76.5% = 23.5% of the original
New Likelihood = 4 × 0.235 = 0.94

Step 8: Round to Risk Scale (1-4)
Risk assessments use a discrete scale from 1 to 4:

- 0.94 rounds to 1
- We ensure it stays between 1 and 4

Residual Likelihood = 1 (Very Unlikely)

Part B: Calculating Impact Reduction

Now we repeat the same process for Impact controls.
Step 1: Convert to Decimals
Impact Controls:

- IDS: 85% = 0.85
- Encryption: 100% = 1.0
- Access Control: 50% = 0.5

Total: 0.85 + 1.0 + 0.5 = 2.35

Step 2: Calculate Average
We have 3 controls affecting impact:
Average Effectiveness = 2.35 ÷ 3 = 0.783 (78.3%)

Step 3: Control Count Multiplier

- Number of controls: 3
- Extra controls: 3 - 1 = 2
- Multiplier: 1.0 + (0.5 × 2) = 2.0

Step 4: Calculate Reduction Factor
Reduction Factor = 0.783 × 2.0 = 1.566

Step 5: Apply 90% Cap
Capped Reduction = minimum of (1.566, 0.90) = 0.90

Step 6: Apply Dampening
Actual Reduction = 0.90 × 0.85 = 0.765 (76.5%)

Step 7: Calculate New Impact
Starting from inherent impact of 4:
Remaining Impact = 100% - 76.5% = 23.5% of original
New Impact = 4 × 0.235 = 0.94

Step 8: Round to Scale
Residual Impact = 1 (Minimal Damage)

Final Result

The Complete Picture:
Before Controls (Inherent Risk):

- Likelihood: 4
- Impact: 4
- Risk Score: 4 × 4 = 16 (Critical)

After Controls (Residual Risk):

- Likelihood: 1
- Impact: 1
- Risk Score: 1 × 1 = 1 (Low)

Risk Level: Low ✅

What This Means

Our layered security controls have successfully reduced a Critical risk (16) down to a Low risk (1).

The controls work together to:
1. Prevent most attacks (Firewall + Encryption + Access Control)
2. Detect breaches quickly (IDS)
3. Minimize damage if an attack succeeds (Encryption + IDS)

Even though one control (Access Control) is degraded to 50% effectiveness, the redundancy provided by having multiple controls ensures the overall risk remains low.

Scenario: What If Access Control Completely Fails?

Let's see what happens if Access Control drops to 0% effectiveness:

Likelihood Recalculation:

Step 2 - New Average:

- Total: 0.9 + 1.0 + 0.0 = 1.9
- Average: 1.9 ÷ 3 = 0.633 (63.3%)

Notice the significant drop from 80% to 63.3%—one failed control is clearly visible.

Step 4 - Reduction Factor:

- 0.633 × 2.0 = 1.266

Step 5 - Cap: 0.90

Step 6 - Dampening: 0.90 × 0.85 = 0.765

Step 7 - New Likelihood: 4 × (1 - 0.765) = 0.94

Step 8 - Rounded: 1

Impact Recalculation:

Using the same math with the failed control: Also rounds to 1

Result with Failed Control:

Residual Risk: 1 × 1 = 1 (Still Low) ✅

Why does the risk stay low?

- We have redundancy (3 controls, not just 1)
- The other two controls are strong (Firewall at 90%, Encryption at 100%)
- Even with one complete failure, average effectiveness (63%) is still reasonable
- The layered defense philosophy protects against single points of failure

However, the degradation is visible in the metrics—the average dropped from 80% to 63%, signaling that action should be taken to restore the failed control.

Key Principles of This Algorithm

1. Layered Defense: Multiple controls provide redundancy—if one fails, others compensate
2. Diminishing Returns: Each additional control adds value, but with decreasing benefit due to overlap
3. Reality Adjustment: The dampening factor (85%) acknowledges that controls never work perfectly in practice
4. Maximum Reduction Cap (90%): Prevents false confidence—risk can never be completely eliminated
5. Visible Degradation: Using average effectiveness makes control failures immediately apparent in the calculations
6. Separate Dimensions: Likelihood and Impact are calculated independently because different control types affect them differently
7. Dynamic Updates: As controls degrade (due to incidents, overdue tasks, or issues), the residual risk automatically increases, prompting corrective action

This algorithm creates a realistic, responsive risk management system that reflects actual operational conditions rather than theoretical assessments.