1. Overview

”is one of the modules of the information security management system (ISMS)”….

2.1.2

Instead of Owner (Admin) – we do Admin

We add the process owner (Process Owner)

2.2

Impact depends on three attributes (C- confidentiality, I- integrity, A- availability)

2.3

The matrix value is up to 25 fields, and they should be consistent with the given colors. It would be nice if the administrator could choose at the implementation stage how many variables he wants to have for the L parameter (from 1 to 5) and how many variables he wants to have for the I parameter (from 1 to 5), i.e. he can choose 5x5 and then he has 25 fields in accordance with the methodology, and if he chooses 3x3 then as you write it can only stay then the maximum risk value is 9 and not 10, here is a simple multiplication:

|  |  |  |
| --- | --- | --- |
| Mother | Risk priorities | Color |
| 2x2 | 1-2 - low | green |
|  | 3-4 high | red |
| 3x3 | 1-4 low | green |
|  | 5-7 medium | blue |
|  | 8-9 high | yellow |
| 4x4 | 1-4 low | green |
|  | 5-8 small | blue |
|  | 9-12 medium | yellow |
|  | 13-16 high | orange |
| 5x5 | 1-4 small | green |
|  | 5-6 low | blue |
|  | 7-10 medium | yellow |
|  | 11-16 high | orange |
|  | 17-25 critical | red |

Remember that in the first move we calculate the risk according to the attached formula for three attributes without any safeguards

Depending on the value of the risk without safeguards, the process owner must perform an action as follows:

|  |  |
| --- | --- |
| Action | Risk Value |
| 2x2 | |
| Accepts and monitors | 1-2 - low |
| Mitigates(implements safeguards) | 3-4 high |
| 3x3 | |
| I accept | 1-4 low |
| Accepts monitors | 5-7 medium |
| I mitigate (I implement safeguards) | 8-9 high |
| 4x4 | |
| Accepts | 1-4 low |
| Akceptuje monitoruje | 5-8 small |
| Mitigates (implements safeguards) | 9-12 medium |
|  | 13-16 high |
| 5x5 | |
| Accepts | 1-4 small |
| Accepts monitors | 5-6 low |
| Mitigates (I implement security) | 7-10 medium |
|  | 11-16 high |
|  | 17-25 critical |

After implementing the security measures, I continue to estimate each attribute separately, but on condition that the risk value after the security measures are implemented reaches a level of 9 …

And then the owner's decision in accordance with the following

|  |  |
| --- | --- |
| I am transferring it to the Management Board, Owner, Supervisory Board, Corporation, etc… | 11-16 high |
| I am closing the process | 17-25 critical |

Remember that when it comes to the name, it is not Risk Assessment itself, but an application for managing information security (I will come up with a name later), Risk is just one of the tiles.