به نام خدا

**عنوان سند:**

# Risk Assessment Methodology

# روش ارزیابی ریسک

## ۱- هدف (Purpose)

هدف از این سند، تعریف یک روش ساخت‌یافته، قابل تکرار و مبتنی بر ریسک برای شناسایی، تحلیل و ارزیابی ریسک‌های امنیت اطلاعات در چارچوب سیستم مدیریت امنیت اطلاعات (ISMS) شرکت «فین‌تک نوآور» می‌باشد. این روش‌شناسی مطابق با الزامات ISO/IEC ۲۷۰۰۱:۲۰۲۲ و همسو با چارچوب‌های NIST CSF و COBIT ۲۰۱۹ تدوین شده است.

## ۲- دامنه کاربرد(Scope)

این روش‌شناسی برای کلیه دارایی‌های اطلاعاتی، فرآیندها، سیستم‌ها، کارکنان و اشخاص ثالث که در دامنه ISMS تعریف شده‌اند، کاربرد دارد و مبنای تصمیم‌گیری برای انتخاب کنترل‌های امنیتی و تدوین برنامه درمان ریسک خواهد بود.

## ۳- تعاریف کلیدی(Definitions)

- **ریسک (Risk)** احتمال وقوع یک تهدید که منجر به بهره‌برداری از آسیب‌پذیری و ایجاد تأثیر منفی بر دارایی اطلاعاتی می‌شود.
- **تهدید (Threat)** عامل بالقوه‌ای که می‌تواند موجب بروز حادثه امنیتی شود.
- **آسیب‌پذیری (Vulnerability)** ضعف یا نقصی که می‌تواند توسط تهدید مورد سوءاستفاده قرار گیرد.
- **مالک ریسک (Risk Owner)** شخص یا واحد مسئول تصمیم‌گیری در خصوص پذیرش یا درمان ریسک.

## ۴- رویکرد کلی ارزیابی ریسک(Risk Assessment Approach)

سازمان از رویکرد کیفی (Qualitative Risk Assessment) برای ارزیابی ریسک استفاده می‌نماید. سطح ریسک بر اساس ترکیب احتمال وقوع و میزان تأثیر تعیین می‌گردد. فرمول محاسبه ریسک:

**Risk Level = Likelihood × Impact**

## ۵- مراحل فرآیند ارزیابی ریسک

### ۵-۱ شناسایی دارایی‌ها

دارایی‌ها بر اساس Asset Inventory شناسایی شده و مالک هر دارایی مشخص می‌گردد.

### ۵-۲ شناسایی تهدیدها و آسیب‌پذیری‌ها

برای هر دارایی، تهدیدهای بالقوه (مانند فیشینگ، دسترسی غیرمجاز، خرابی سیستم) و آسیب‌پذیری‌های مرتبط شناسایی می‌شوند.

### ۵-۳ تحلیل ریسک

برای هر سناریوی ریسک، احتمال وقوع و میزان تأثیر بر اساس معیارهای تعریف‌شده امتیازدهی می‌گردد.

### ۵-٤ ارزیابی و اولویت‌بندی ریسک

سطح ریسک محاسبه شده و ریسک‌ها بر اساس میزان بحرانی بودن اولویت‌بندی می‌شوند.

### ۵-۵ تعیین مالک ریسک

برای هر ریسک، یک مالک مشخص می‌شود که مسئول پیگیری اقدامات درمان ریسک خواهد بود.

## ۶- معیار احتمال وقوع(Likelihood Criteria)

| امتیاز | توضیح |
|---|---|
| 1 | بسیار کم – وقوع نادر |
| 2 | کم – وقوع غیرمحتمل |
| 3 | متوسط – وقوع ممکن |
| 4 | زیاد – وقوع محتمل |
| 5 | بسیار زیاد – وقوع مکرر |

## ۷- معیار تأثیر(Impact Criteria)

| امتیاز | توضیح |
|---|---|
| 1 | تأثیر ناچیز، بدون اختلال قابل توجه |
| 2 | تأثیر کم، اختلال محدود |
| 3 | تأثیر متوسط، اختلال قابل توجه در سرویس |
| 4 | تأثیر زیاد، توقف سرویس یا جریمه قانونی |
| 5 | تأثیر بسیار زیاد، خسارت مالی/اعتباری شدید |

## ۸- ماتریس ارزیابی ریسک(Risk Matrix)

| Impact \ Likelihood | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **5** | 5 | 10 | 15 | 20 | 25 |
| **4** | 4 | 8 | 12 | 16 | 20 |
| **3** | 3 | 6 | 9 | 12 | 15 |
| **2** | 2 | 4 | 6 | 8 | 10 |
| **1** | 1 | 2 | 3 | 4 | 5 |

سطوح ریسک به‌صورت زیر تفسیر می‌شوند:

- **Low (1–5):** قابل پذیرش
- **Medium (6–12):** نیازمند اقدام کنترلی
- **High (15–25):** غیرقابل پذیرش و نیازمند درمان فوری

## ۹- معیار پذیرش ریسک Risk Acceptance Criteria

ریسک‌های باقی‌مانده (Residual Risks) که در سطح Low یا Medium قرار دارند، با تأیید مدیریت ارشد قابل پذیرش خواهند بود. پذیرش ریسک‌ها مستندسازی می‌گردد.

## ۱۰- خروجی‌های فرآیند ارزیابی ریسک

- Risk Register
- Risk Treatment Plan
- Statement of Applicability (SoA)

## ۱۱- پایش و بازبینی

ارزیابی ریسک حداقل سالی یک‌بار و همچنین در صورت تغییرات اساسی در دارایی‌ها، فناوری، تهدیدات یا دامنه ISMS بازبینی می‌گردد.

تصویب‌کننده :مدیریت ارشد شرکت

تاریخ اجرا

نسخه