

## فهرست مطالب

۳	پیشگفتار
۷	معرفی
۱۵	۴. بافتار سازمان
۱۵	۱.۴ شناخت سازمان و بافتار آن
۲۳	۲.۴ درک نیازها و انتظارات طرف‌های علاقه‌مند
۲۵	۳.۴ تعیین محدوده (دامنه) سیستم مدیریت امنیت اطلاعات
۳۱	۴.۴ سیستم مدیریت امنیت اطلاعات
۳۳	۵ رهبری
۳۳	۱.۵ رهبری و تعهد
۳۹	۲.۵ خط‌مشی
۴۵	۳.۵ نقش‌ها، مسئولیت‌ها و اختیارات سازمانی
۴۹	۶ طرح‌ریزی
۴۹	۱.۶ اقدامات جهت پرداختن به مخاطرات و فرصت‌ها
۴۹	۱.۱.۶ کلیات
۵۷	۲.۱.۶ ارزیابی مخاطرات امنیت اطلاعات
۷۱	۳.۱.۶ برطرف‌سازی مخاطرات امنیت اطلاعات
۸۷	۲.۶ اهداف امنیت اطلاعات و طرح‌ها برای دستیابی به آنها
۹۹	۷ پشتیبانی
۹۹	۱.۷ منابع
۱۰۳	۲.۷ شایستگی
۱۰۷	۳.۷ آگاه‌سازی
۱۱۱	۴.۷ ارتباطات
۱۱۹	۵.۷ اطلاعات مستند
۱۱۹	۱.۵.۷ کلیات
۱۲۵	۲.۵.۷ ایجاد و به‌روزرسانی
۱۳۱	۳.۵.۷ کنترل اطلاعات مستند
۱۳۵	۸ عملیات
۱۳۵	۱.۸ طرح‌ریزی و کنترل عملیات
۱۴۳	۲.۸ ارزیابی مخاطرات امنیت اطلاعات
۱۴۵	۳.۸ برطرف‌سازی مخاطرات امنیت اطلاعات
۱۴۹	۹ ارزشیابی عملکرد
۱۴۹	۱.۹ پایش، اندازه‌گیری، تحلیل و ارزشیابی
۱۵۵	۲.۹ ممیزی داخلی
۱۶۷	۳.۹ بازنگری مدیریت
۱۷۵	۱۰ بهبود
۱۷۵	۱.۱۰ عدم انطباق و اقدامات اصلاحی
۱۸۷	۲.۱۰ بهبود مستمر
۱۹۵	پیوست A
۲۰۵	کتابنامه
۲۰۶	چک لیست ممیزی بندهای ۴ تا ۱۰ از استاندارد ISO/IEC 27001:2013

**content**

Foreword.....	4
Introduction .....	8
4.2 Understanding the needs and expectations of interested parties .....	24
4.4 Information security management system .....	32
5 Leadership .....	34
5.1 Leadership and commitment.....	34
5.2 Policy.....	40
5.3 Organizational roles, responsibilities and authorities.....	46
6 Planning.....	50
6.1 Actions to address risks and opportunities.....	50
6.1.1 General .....	50
6.1.2 Information security risk assessment .....	58
6.1.3 Information security risk treatment.....	72
6.2 Information security objectives and planning .....	88
7 Support .....	100
7.1 Resources.....	100
7.2 Competence .....	104
7.3 Awareness.....	108
7.4 Communication .....	112
7.5 Documented information .....	120
7.5.1 General .....	120
7.5.2 Creating and updating.....	126
7.5.3 Control of documented information.....	132
8 Operation .....	136
8.1 Operational planning and control.....	136
8.2 Information security risk assessment .....	144
8.3 Information security risk treatment.....	146
9 Performance evaluation .....	150
9.1 Monitoring, measurement, analysis and evaluation .....	150
9.2 Internal audit.....	156
9.3 Management review.....	168
10 Improvement.....	176
10.1 Nonconformity and corrective action.....	176
10.2 Continual improvement .....	188
Annex A .....	196