INSO –ISO-IEC
10164-8

1st. Edition

Identical with
ISO/IEC 10164-8:
1993+ Cor1:1995 +
Cor2:1996 + Cor3:1999
Jun.2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ایران - ایزو آی ای سی

۱۰۱۶۴-۸

چاپ اول

خرداد ۱۳۹۲

فناوری اطلاعات- اتصال متقابل سامانه‌های باز- مدیریت سامانه‌ها: کارکرد دنباله ممیزی امنیت

Information technology - Open Systems Interconnection - Systems Management: Security audit trail function

ICS:35.100.70

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- اتصال متقابل سامانه‌های باز- مدیریت سامانه‌ها: کارکرد دنباله ممیزی امنیت»

رئیس:	**سمت یا نمایندگی**
رضایی، رامین (لیسانس مهندسی برق - الکترونیک)	معاون طرح و توسعه مرکز تحقیقات صنایع انفورماتیک
دبیر:	
منافی، علیرضا (فوق لیسانس مهندسی معماری کامپیوتر)	معاون فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک
اعضاء: (اسامی به ترتیب حروف الفبا)	
افکار، علی (دکترای مهندسی برق- الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت
ترابی، سعید (لیسانس مدیریت صنعتی)	مدیر فنی شرکت بازرسی کالای تجاری
تورانی، فرزام (لیسانس مهندسی کامپیوتر)	کارشناس مرکز تحقیقات صنایع انفورماتیک
فرج‌پور، مهیار (فوق لیسانس مهندسی برق - الکترونیک)	عضو هیات مدیره شرکت سیماوا
فرخی، علی (دکتری مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه آزاد اسلامی تهران جنوب
زندباف، عباس (لیسانس مهندسی الکترونیک - مخابرات)	کارشناس شرکت ارتباطات زیرساخت
نادری، مجید (دکترای مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت

فهرست مندرجات

پیش‌گفتار

استاندارد "فناوری اطلاعات- اتصال متقابل سامانه‌های باز- مدیریت سامانه‌ها: کارکرد دنباله ممیزی امنیت " که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکز تحقیقات صنایع انفورماتیک، بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه‌ای یا ملی استانداردهای "بین‌المللی/ منطقه‌ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران، تهیه شده و در یک صد و پنجاه و چهارمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۰/۱۰/۱۸ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آنها استفاده خواهد شد.

این استاندارد ملی براساس پذیرش استاندارد بین‌المللی به شرح زیر است :

ISO/IEC 10164-8:1993 + Cor1:1995 + Cor2:1996 + Cor3:1999 (E), Information technology - Open Systems Interconnection - Systems Management: Security Audit trail function

فناوری اطلاعات- اتصال متقابل سامانه‌های باز- مدیریت سامانه‌ها: کارکرد دنباله ممیزی امنیت

۱ هدف و دامنه کاربرد

این استاندارد ملی براساس پذیرش استاندارد بین‌المللی ISO/IEC 10164-8: 1993 + Cor1:1995 + Cor3:1999 + Cor2:1996 تدوین شده است.

هدف از تدوین این استاندارد تعریف عملکرد دنباله ممیزی امنیت است. عملکرد دنباله ممیزی امنیت، یک نوع عملکرد مدیریت سامانه‌هاست که همانطوریکه در استاندارد CCITT Rec. X.700 | ISO/IEC 7498-4 تعریف شده است، می‌تواند توسط یک فرایند کاربردی در محیط مدیریتی متمرکز یا غیرمتمرکز برای تبادل اطلاعات به‌منظور مدیریت سامانه‌ها به‌کار گرفته شوند. این عملکرد در لایه کاربرد استاندارد CCITT Rec. X.200 | ISO/IEC 7498 قرار گرفته است و طبق مدل آماده شده توسط استاندارد ISO/IEC 9545 تعریف می‌شود. نقش عملکردهای مدیریت سامانه در استاندارد CCITT Rec. X.701 | ISO/IEC 10040 شرح داده شده است.

این استاندارد به موضوعات ذیل می‌پردازد:

- الزامات کاربر برای تعریف خدمتی که برای پشتیبانی از عملکرد گزارش دنباله ممیزی امنیت مورد نیاز است را وضع می‌کند.
- خدمات فراهم شده توسط عملکرد گزارش دنباله ممیزی امنیت را تعریف می‌کند.
- پروتکل لازم برای آماده سازی خدمت را مشخص می‌کند.
- رابطه بین سرویس و اعلانیه های مدیریت را تعریف می‌کند.
- ارتباطات با عملکردهای مدیریت سامانه‌های دیگر را تعریف می‌کند.
- الزامات انطباق را مشخص می‌کند.

این استاندارد موارد زیر را دربر نمی‌گیرد:

- ممیزی امنیت یا چگونگی انجام آن. یک ممیزی امنیت می‌تواند برای کمک به تخمین اثرگذاری خط مشئ امنیت مورد استفاده قرار گیرد. خط‌مشئ امنیت طبقه‌بندی رویدادهای مرتبط با امنیت که نیاز به ممیزی دارند و محل ثبت گزارش دنباله ممیزی امنیت را که در آن ضبط خواهند شد، مشخص می‌کند.
- طبیعت هر فعالیتی که به منظور فراهم آوردن عملکرد دنباله ممیزی امنیت انجام شده باشد.
- مواقعی که استفاده از عملکرد دنباله ممیزی امنیت مناسب است.
- خدماتی که برای وضع و واگذاری عادی و غیرعادی انجمن مدیریت لازم است.

– هر هشدار دیگر تعریف شده توسط استانداردهای بین‌المللی که باب میل مدیر امنیت باشد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد ملی الزامی است : [۱]

2-1 CCITT Recommendation X.701 (1992) | ISO/IEC 10040:1992, Information technology - Open Systems Interconnection - Systems management overview.[2]

2-2 CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2:1992, Information technology - Open Systems Interconnection – Structure of management information: Definition of management information.

2-3 CCITT Recommendation X.722 (1992) | ISO/IEC 10165-4:1992, Information technology - Open Systems Interconnection – Structure of management information: Guidelines for the definition of managed objects.

2-4 CCITT Recommendation X.724 | ISO/IEC 10165-4, Information technology - Open Systems Interconnection – Structure of management information: Requirements and guidelines for implementation conformance Statement proformas associated with management information.

2-5 CCITT Recommendation X.733 (1992) | ISO/IEC 10164-4:1992, Information technology - Open Systems Interconnection – Systems Management: Alarm reporting function.

2-6 CCITT Recommendation X.734 (1992) | ISO/IEC 10164-5:1992, Information technology - Open Systems Interconnection – Systems Management: Event report management function.

2-7 CCITT Recommendation X.735 (1992) | ISO/IEC 10164-6:1992, Information technology - Open Systems Interconnection - Systems Management: Log control function.

2-8 CCITT Recommendation X.736 (1992) | ISO/IEC 10164-7:1992, Information technology - Open Systems Interconnection - Systems Management: Security alarm reporting function.

2-9 ITU-T Recommendation X.724 (1993) | ISO/IEC 10165-6:1994, Information technology - Open Systems Interconnection - Structure of management information:

---

۱ - مراجع الزامی ردیف‌های ۲-۱ الی ۲-۹ توصیه نامه| استانداردهای بین‌المللی همسان هستند. مراجع الزامی ردیف‌های ۲-۱۰الی ۲-۲۹ زوج توصیه نامه| استانداردهای بین‌المللی هستند که از لحاظ محتویات فنی معادلندو مرجع الزامی ردیف‌های ۲-۳۰ و ۲-۳۱ مراجع افزونه هستند.

۲ - همانطور که توسط استاندارد "ITU-T Rec. X.701Kor.2 I ISO/IEC 10040Kor.2" اصلاح شده است.

Requirements and guidelines for implementation conformance statement proformas associated with OSI management.

2-10 CCITT Recommendation X.200 (1988), Reference Model of Open Systems Interconnection for CCITT Applications.

2-11 ISO 7498:1984, Information processing systems - Open Systems Interconnection – Basic Reference Model.

2-12 CCITT Recommendation X.208 (1988), Specification of Abstract Syntax Notation One (ASN.1).

2-13 ISOIIEC 8824:1990, Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).

2-14 CCITT Recommendation X.209 (1988), Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1).

2-15 ISO/IEC 8825:1990, Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

2-16 CCITT Recommendation X.210 (1988), Open Systems Interconnection. Layer Service Definition Conventions.

2-17 ISO/TR 8509:1987, Information processing systems - Open Systems Interconnection – Service conventions

2-18 CCITT Recommendation X.290 (1992), OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications - General concepts.

2-19 ISO/IEC 9646-1: 1991, Information technology - Open Systems Interconnection – Conformance testing methodology and framework - Part 1: General concepts.

2-20 CCITT Recommendation X.291 (1992), OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications - Abstract test Suite specification.

2-21 ISOIIEC 9646-2: 1991, Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract test Suite specification.

2-22 CCI'IT Recommendation X.700 (1992), Management Framework Definition for Open Systems Interconnection (OSI) for CCITT Applications.

2-23 ISO/IEC 7498-4:1989, Information processing systems - Open Systems Interconnection – Basic Reference Model - Part 4: Management framework.

2-24 CCITT Recommendation X.710 (1991), Common Management Information Service Definition for CCITT applications.

2-25 ISO/IEC 9595:1991, Information technology - Open Systems Interconnection – Common management information service definition.

2-26 CCITT Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

2-27 ISO 7498-2: 1989, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security architecture.

2-28 ITU-T Recommendation X.2961, OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications - Implementation conformance Statements.

---

۱ - در حال حاضر در مرحله پیش نویس است.

2-29 ISO/IEC 9646-7 1, Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements.

2-30 ISO/IEC 9545:1989, Information technology - Open Systems Interconnection - Application layer structure.

2-31 ISO/IEC 10181-7, Information technology - Open Systems Interconnection - Security frameworks - Part 7: Security audit framework.

کلیه‌ی بندهای استاندارد بین‌المللی ISO/IEC 10164-8: 1993 + Cor1:1995 + Cor2:1996 + Cor3:1999 در مورد این استاندارد معتبر و الزامی است.