٩. الملحق

I. نطاق الملحق

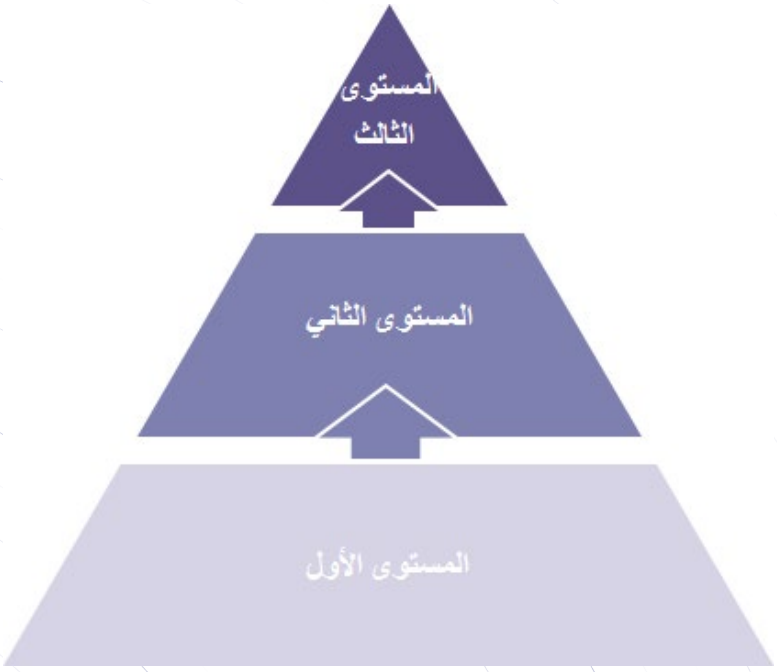
يختص هذا الملحق بتوضيح مستهدفات الالتزام، وهيكلية المتطلبات والضوابط المتعلقة بمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة.

II. مستهدفات الالتزام

تقوم الهيئة بوضع مستهدفات الالتزام من خلال تحديد ثلاث مستويات باتباع منهجية قائمة على إدارة المخاطر، ويحتوي كل مستوى على مجموعة من ضوابط الأمن السيبراني، وتختلف المستويات الثلاثة في متطلبات الضوابط:

- المستوى الأول: يشمل متطلبات الحد الأدنى من الضوابط.
- المستوى الثاني: يشمل متطلبات متقدمة من الضوابط.
- المستوى الثالث: يشمل متطلبات تعمل على مراقبة الكفاءة والتحسين المستمر لضوابط المستويين الأول والثاني.

تحقيق الالتزام بأحد المستويات يتطلب تحقيق الالتزام بالمستويات السابقة.



الشكل ١ - مستويات الالتزام

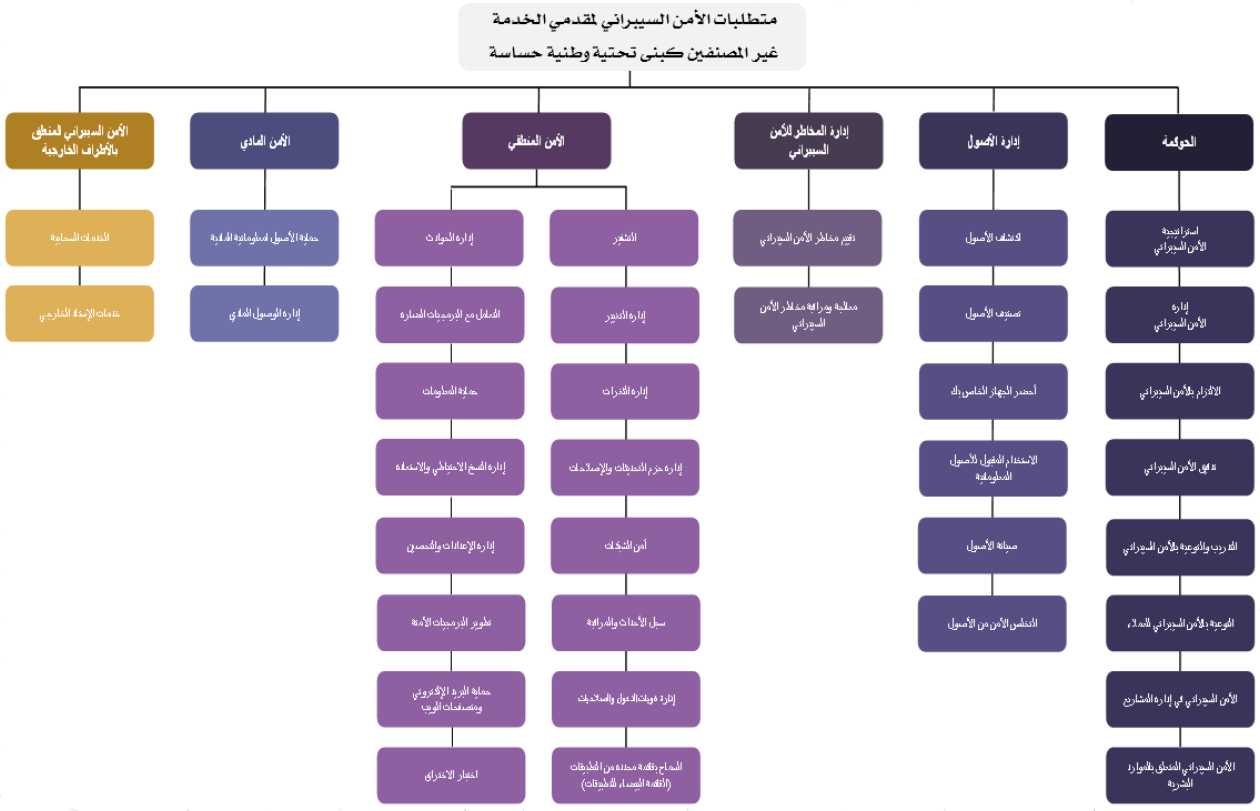
تشتمل مستهدفات الالتزام لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة على مستوى الالتزام المطلوب وتاريخه، وهو ما سيتم تحديده والرفع به رسمياً من قبل الهيئة.

III. هيكلية المتطلبات

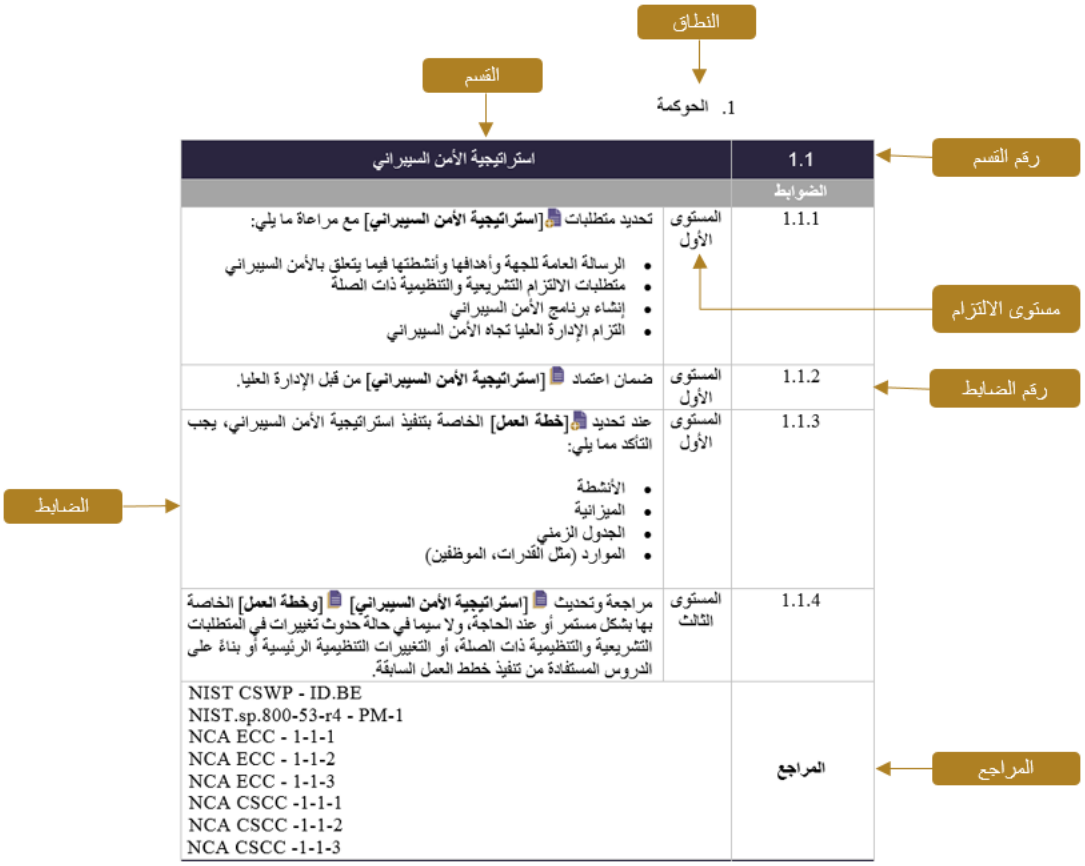
تنقسم متطلبات الأمن السيبراني لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة إلى ست نطاقات:

الشكل ٢ - نطاقات متطلبات الأمن السيبراني لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة

تم تقسيم كل نطاق إلى أقسام أكثر تخصصاً تجمع ضوابط الأمن السيبراني ذات الصلة بالموضوع المحدد وتشترك في نفس الهدف.



الشكل ٣ - نطاقات وأقسام متطلبات الأمن السيبراني لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة



1.1	استراتيجية الأمن السيبراني	
الضوابط		
1.1.1	المستوى الأول	تحديد متطلبات [استراتيجية الأمن السيبراني] مع مراعاة ما يلي: • الرسالة العامة للجهة وأهدافها وأنشطتها فيما يتعلق بالأمن السيبراني • متطلبات الالتزام التشريعية والتنظيمية ذات الصلة • إنشاء برنامج الأمن السيبراني • التزام الإدارة العليا تجاه الأمن السيبراني
1.1.2	المستوى الأول	ضمان اعتماد [استراتيجية الأمن السيبراني] من قبل الإدارة العليا.
1.1.3	المستوى الأول	عند تحديد [خطة العمل] الخاصة بتنفيذ استراتيجية الأمن السيبراني، يجب التأكد مما يلي: • الأنشطة • الميزانية • الجدول الزمني • الموارد (مثل القدرات، الموظفين)
1.1.4	المستوى الثالث	مراجعة وتحديث [استراتيجية الأمن السيبراني] [وخطة العمل] الخاصة بها بشكل مستمر أو عند الحاجة، ولا سيما في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة، أو التغييرات التنظيمية الرئيسية أو بناءً على الدروس المستفادة من تنفيذ خطط العمل السابقة.
المراجع	NIST CSWP - ID.BE NIST.sp.800-53-r4 - PM-1 NCA ECC - 1-1-1 NCA ECC - 1-1-2 NCA ECC - 1-1-3 NCA CSCC -1-1-1 NCA CSCC -1-1-2 NCA CSCC -1-1-3	

الشكل ٤ - هيكل المتطلبات

ملاحظات هامة

يتم ترميز معلومات الضابط الخاصة على سبيل المثال: [العمليات]، و[المُخرجات]، و[المراجع] (على سبيل المثال فيما يتعلق بغيرها من الضوابط والأقسام والعمليات ووثائق الهيئة) بشكل منفصل في كافة أجزاء المتطلبات. عند التطابق، يتم أيضًا تظليل اعتبارات الضابط [الخاصة بالاتصالات وتقنية المعلومات والبريد].

ترتبط الضوابط الواردة في المتطلبات ببعضها البعض، فعلى سبيل المثال يمكن أن تكون نتيجة ضابط ما في قسم ما مدخلًا لضابط آخر في قسم مختلف (على سبيل المثال يعمل [تقرير الثغرات] الذي يتم إعداده في قسم إدارة الثغرات الأمنية كمدخل إلى قسم إدارة حزم التحديثات والإصلاحات).

تغطي العمليات والمخرجات المُظللة أبرز تدابير الأمن السيبراني وليس بالضرورة جميعها. حيث أنها تهدف للتركيز على العمليات والمخرجات المتوقعة من أجل تحسين قابلية استخدام ضوابط المتطلبات ووضوحها.

فيما يلي الرموز المستخدمة في المتطلبات وتفسيراتها:


مُخرج جديد


مُخرج


عملية جديدة


عملية


مرجع


الاعتبارات الخاصة بالاتصالات وتقنية المعلومات والبريد

IV. المراجع

أخذت الهيئة في الاعتبار الإسهامات المتوفرة من عدد من المعايير والأطر واللوائح المرتبطة بالأمن السيبراني والأعمال المماثلة التي أعدتها جهات تنظيمية أخرى حيث تمت مراعاة المراجع التالية أثناء وضع الإطار التنظيمي:

- ISO/IEC 27001 (2013)
- ISO/IEC 27002 (2013)
- ISO 27011/ITU-T X.1051 (2016)
- ISO/IEC 27004 (2016)
- ITU-T X series
- SANS CIS Critical Security Controls Version 6.1 (2016) and 7 (2018)
- National Institute of Standards & Technologies: Framework for Improving Critical Infrastructure Cybersecurity (NIST CSWP, 2018)
- National Institute of Standards & Technologies: Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Revision 4, (2013)
- الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني (٢٠١٨)
- وضوابط الأمن السيبراني للأنظمة الحساسة الصادرة عن الهيئة الوطنية للأمن السيبراني (٢٠١٨)


CITC
هيئة الاتصالات وتقنية المعلومات
Communications & Information
Technology Commission
CITC_SA
CITC.SA
www.citc.gov.sa