٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience aspects of Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجهة. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.
الضوابط	
٣-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة.
٣-١-٢	يجب تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة.
٣-١-٣	يجب أن تغطي إدارة استمرارية الأعمال في الجهة بحد أدنى ما يلي: ٣-١-٣-١ التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني. ٣-١-٣-٢ وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة. ٣-١-٣-٣ وضع خطط التعافي من الكوارث (Disaster Recovery Plan).
٣-١-٤	يجب مراجعة متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة دورياً.