NIST SP 800-161 R1 Controls

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Tier 1	Tier 2	Tier 3	Prioritized Implementation Plan Phase #
AC-1	Policy and Procedures	AC-1	AC-1	AC-1	AC-1	AC-1	4
AC-2	Account Management	AC-2	AC-2		AC-2	AC-2	14
AC-3	Access Enforcement	AC-3	AC-3		AC-3	AC-3	14
AC-3(8)	Access Enforcement | Revocation of Access Authorizations				AC-3(8)	AC-3(8)	14
AC-3(9)	Access Enforcement | Controlled Release				AC-3(9)	AC-3(9)	14
AC-4	Information Flow Enforcement		AC-4		AC-4	AC-4	15
AC-4(6)	Information Flow Enforcement | Metadata				AC-4(6)	AC-4(6)	15
AC-4(17)	Information Flow Enforcement | Domain Authentication				AC-4(17)	AC-4(17)	15
AC-4(19)	Information Flow Enforcement | Validation of Metadata				AC-4(19)	AC-4(19)	15
AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows					AC-4(21)	15
AC-5	Separation of Duties		AC-5		AC-5	AC-5	14
AC-6(6)	Least Privilege | Privileged Access by Non- organizational Users				AC-6(6)	AC-6(6)	14
AC-17	Remote Access	AC-17	AC-17		AC-17	AC-17	15
AC-17(6)	Remote Access | Protection of Mechanism Information				AC-17(6)	AC-17(6)	15
AC-18	Wireless Access	AC-18		AC-18	AC-18	AC-18	15
AC-19	Access Control for Mobile Devices	AC-19			AC-19	AC-19	15
AC-20	Use of External Systems	AC-20	AC-20	AC-20	AC-20	AC-20	9
AC-20(1)	Use of External Systems | Limits on Authorized Use				AC-20(1)	AC-20(1)	9
AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use				AC-20(3)	AC-20(3)	9
AC-21	Information Sharing			AC-21	AC-21		24
AC-22	Publicly Accessible Content	AC-22			AC-22	AC-22	24
AC-23	Data Mining Protection		AC-23		AC-23	AC-23	10
AC-24	Access Control Decisions		AC-24	AC-24	AC-24	AC-24	24
AT-1	Policy and Procedures	AT-1		AT-1	AT-1		4
AT-2(1)	Literacy Training and Awareness | Practical Exercises				AT-2(1)		20
AT-2(2)	Literacy Training and Awareness | Insider Threat	AT-2(2)	AT-2(2)		AT-2(2)		20
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining				AT-2(3)		20
AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior				AT-2(4)		20
AT-2(5)	Literacy Training and Awareness | Advanced Persistent Threat				AT-2(5)		20
AT-2(6)	Literacy Training and Awareness | Cyber Threat Environment				AT-2(6)		20
AT-3	Role-based Training	AT-3	AT-3		AT-3		20
AT-3(2)	Role-based Training | Physical Security Controls				AT-3(2)		20
AT-4	Training Records	AT-4			AT-4		20
AU-1	Policy and Procedures	AU-1		AU-1	AU-1	AU-1	4
AU-2	Event Logging	AU-2	AU-2	AU-2	AU-2	AU-2	13
AU-3	Content of Audit Records	AU-3	AU-3	AU-3	AU-3	AU-3	13
AU-6	Audit Record Review, Analysis, and Reporting	AU-6			AU-6	AU-6	13
AU-6(9)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Non-technical Sources					AU-6(9)	13
AU-10	Non-repudiation					AU-10	14
AU-10(1)	Non-repudiation | Association of Identities				AU-10(1)		14
AU-10(2)	Non-repudiation | Validate Binding of Information Producer Identity				AU-10(2)	AU-10(2)	14
AU-10(3)	Non-repudiation | Chain of Custody				AU-10(3)	AU-10(3)	14
AU-12	Audit Record Generation	AU-12	AU-12		AU-12	AU-12	13
AU-13	Monitoring for Information Disclosure		AU-13		AU-13	AU-13	13
AU-14	Session Audit		AU-14		AU-14	AU-14	13
AU-16	Cross-organizational Audit Logging				AU-16	AU-16	13
AU-16(2)	Cross-organizational Audit Logging | Sharing of Audit Information		AU-16(2)		AU-16(2)	AU-16(2)	13
CA-1	Policy and Procedures	CA-1		CA-1	CA-1	CA-1	4
CA-2	Control Assessments	CA-2			CA-2	CA-2	22
CA-2(2)	Control Assessments | Specialized Assessments					CA-2(2)	22
CA-2(3)	Control Assessments | Leveraging Results from External Organizations					CA-2(3)	22
CA-3	Information Exchange	CA-3	CA-3			CA-3	15
CA-5	Plan of Action and Milestones	CA-5			CA-5	CA-5	7c
CA-6	Authorization	CA-6		CA-6	CA-6	CA-6	22
CA-7(3)	Continuous Monitoring | Trend Analyses					CA-7(3)	13
CM-1	Policy and Procedures	CM-1		CM-1	CM-1	CM-1	4
CM-2	Baseline Configuration	CM-2	CM-2		CM-2	CM-2	10
CM-2(6)	Baseline Configuration | Development and Test Environments				CM-2(6)	CM-2(6)	10
CM-3	Configuration Change Control		CM-3		CM-3	CM-3	9
CM-3(1)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes				CM-3(1)	CM-3(1)	9
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes				CM-3(2)	CM-3(2)	9
CM-3(4)	Configuration Change Control | Security and Privacy Representatives				CM-3(4)	CM-3(4)	9
CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes				CM-3(8)	CM-3(8)	9
CM-4	Impact Analyses	CM-4				CM-4	9

Cybersecurity Supply Chain Risk Management (C-SCRM) Geographic Risk Management

Region	Country	CPI Score [2021]	Host Country Data Localization Laws	301 Report [as of 2022]		Designated State Sponsors of Terrorism [as of 2022]	Notorious Markets List [as of 2021]	Export Administration Regulations (EAR) [as of 2 June 2022]							Risk Management Tier Approval & Prohibition Considerations
				Priority Watch List	Watch List			D:1	D:2	D:3	D:4	D:5	E:1	E:2	
APAC	Afghanistan	16								X		X			Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
EMEA	Albania	35													Level 2 (Senior Management) review: high corruption risk
EMEA	Algeria	33			X										Level 2 (Senior Management) review: IP risk | high corruption risk
APAC	American Samoa	N/A													
EMEA	Andorra	N/A													
EMEA	Angola	29													Level 2 (Senior Management) review: high corruption risk
AMER	Anguilla	N/A													
N/A	Antarctica	N/A													
AMER	Antigua and Barbuda	N/A													
AMER	Argentina	38		X			X								Level 2 (Senior Management) review: IP risk | high corruption risk
EMEA	Armenia	49						X		X					Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
AMER	Aruba	N/A													
APAC	Australia	73													
EMEA	Austria	74													
EMEA	Azerbaijan	30						X		X					Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
AMER	Bahamas	64													Level 1 (Line Management) review: moderate corruption risk
EMEA	Bahrain	42								X	X				Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
APAC	Bangladesh	26													Level 2 (Senior Management) review: high corruption risk
AMER	Barbados	65			X										Level 2 (Senior Management) review: IP risk | moderate corruption risk
EMEA	Belarus	41						X	X	X	X	X			Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
EMEA	Belgium	73													
AMER	Belize	N/A													
EMEA	Benin	42													Level 2 (Senior Management) review: high corruption risk
AMER	Bermuda	N/A													
APAC	Bhutan	68													Level 1 (Line Management) review: moderate corruption risk
AMER	Bolivia	30			X										Level 2 (Senior Management) review: IP risk | high corruption risk
AMER	Bonaire, Sint Eustatius and Saba	N/A													
EMEA	Bosnia and Herzegovina	35													Level 2 (Senior Management) review: high corruption risk
EMEA	Botswana	55													Level 1 (Line Management) review: moderate corruption risk
AMER	Bouvet Island	N/A													
AMER	Brazil	38			X		X								Level 2 (Senior Management) review: IP risk | high corruption risk
EMEA	British Indian Ocean Territory	N/A													
AMER	British Virgin Islands	N/A													
APAC	Brunei	N/A													
EMEA	Bulgaria	42													Level 2 (Senior Management) review: high corruption risk
EMEA	Burkina Faso	42													Level 2 (Senior Management) review: high corruption risk
EMEA	Burundi	19													Level 2 (Senior Management) review: high corruption risk
EMEA	Cabo Verde	N/A													
APAC	Cambodia	23					X	X				X			Level 3 (Executive Management) review: ITAR/EAR compliance review | IP risk | high corruption risk
EMEA	Cameroon	27													Level 2 (Senior Management) review: high corruption risk
AMER	Canada	74			X		X								Level 2 (Senior Management) review: IP risk
AMER	Cayman Islands	N/A													
EMEA	Central African Republic	24										X			Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
EMEA	Chad	20													Level 2 (Senior Management) review: high corruption risk
AMER	Chile	67		X											Level 2 (Senior Management) review: IP risk | moderate corruption risk
APAC	China	45	Data Security Law China Privacy Law				X	X		X	X	X			Level 4 (Board of Directors) review: ITAR/EAR compliance review | IP risk | high corruption risk | restrictive data localization requirements
APAC	China, Hong Kong	76													
APAC	China, Macao	N/A						X		X	X				Level 3 (Executive Management) review: ITAR/EAR compliance review
APAC	Christmas Island	N/A													
APAC	Cocos (Keeling) Islands	N/A													
AMER	Colombia	39			X										Level 2 (Senior Management) review: IP risk | high corruption risk
EMEA	Comoros	20													Level 2 (Senior Management) review: high corruption risk
EMEA	Congo	21										X			Level 3 (Executive Management) review: ITAR/EAR compliance review | high corruption risk
APAC	Cook Islands	N/A													
AMER	Costa Rica	58													Level 1 (Line Management) review: moderate corruption risk
EMEA	Côte d'Ivoire	36													Level 2 (Senior Management) review: high corruption risk
EMEA	Croatia	47													Level 2 (Senior Management) review: high corruption risk
AMER	Cuba	46				X			X	X		X		X	Level 4 (Board of Directors) review: prohibited country | high corruption risk
AMER	Curaçao	N/A													
EMEA	Cyprus	53										X			Level 3 (Executive Management) review: ITAR/EAR compliance review | moderate corruption risk
EMEA	Czech Republic	54													Level 1 (Line Management) review: moderate corruption risk
EMEA	Democratic Republic of the Congo	19													Level 2 (Senior Management) review: high corruption risk
EMEA	Denmark	88													
EMEA	Djibouti	30													Level 2 (Senior Management) review: high corruption risk