Stepping Through Cybersecurity Risk Management

Cybersecurity Risk Management Acronyms

Author: Jennifer L. Bayuk

Acronym	Expansion
ACM	Access Control Matrix
AI	Artificial Intelligence
AIV	Application Input Validation
APT	Advanced Persistent Threat
ATT&CK	MITRE's registered trademark for a knowledge base of attack patterns
AV	Anti-Virus
BEC	Business Email Compromise
BEICF	Business Environment And Internal Control Factors
C&C	Command & Control
CAPEC	Common Attack Pattern Enumeration and Classification
CAT	Cybersecurity Assessment Tool
CCF	Common Cause Failure
CEO	Chief Executive Officer
CIO	Chief Information Officier
CIS	Center For Internet Security
CISA	Cyber and Infrastructure Security Agency
CISO	Chief Information Security Officier
CMDB	Configuration Management DataBase
COBIT	Control Objectives for Information Technology
COBOL	Common Business Oriented Language
COO	Chief Operations Officer
COSO	Committee on Sponsoring Organizations of the Treadway Comission
COTS	Commerical Off The Shelf
CPE	Standardized Product Names
CRO	Chief Risk Officer
CSF	Cybersecurity Framework
CVE	Common Vulnerability Enumeration
CVE	Common Vulnerabilities and Exposure

Acronym	Expansion
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CXO	the highest ranked person in job function within their organization
DBMS	DataBase Management System
DBT	Design Basis Threat
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DSS	Deliver Service and Support
EDR	Endpoint Detection & Response
EMT	Emergency Medical Technician
ERP	Enterprise Resource Planning
EU GDPR	European Union's General Data Protection Regulation
FFIEC	Federal Financial Institutions Examination Council
FMECA	Failure Modes, Effects, & Criticality Analysis
FS-ISAC	Financial Industry Information Sharing and Analysis Center
FTC	Federal Trade Commission
GQM	Goal Question Metric
GRC	Governance, Risk and Compliance (originally Governance, Risk and Control)
GRU	Russia's General Staff Main Intelligence Directorate
GTsST	Russia's Main Center for Special Technologies
HIPAA	Health Insurance Portability & Accountability Act
HR	Human Resources
HW	Hardware
IAM	Identity & Access Management
IAM-SO	Identity & Access Management Service Owner
ID	Identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INCOSE	International Council On Systems Engineering
IP	Internet Protocol
ISACA	Formerly the Information Systems Audit & Control Association, and before that, the EDP Auditor's Association, now just an acronym for a name
ISMS	Information Security Management System
ISO	International Standards Organization
IT	Information Technology

Acronym	Expansion
ITIL	Information Technology Infrastructure Library
JML	Joiners, Movers, Leavers
KEV	Known Exploited Vulnerability
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KXI	Key Indicator of type
MAC	Media Access Control
MFA	MultiFactor Authentication
MIT	Massachusetts Institute of Technology
MITRE	a corporate name that intentionally means nothing, no expansion available
NACD	National Association of Corporate Directors
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OASIS	Organization for the Advancement of Structured Information Standards
OODA	Observe, Orient, Decide, Act
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
POC	Proof Of Concept
PPSP	Policies, Processes, Standards, And Procedures
RACI	Responsible, Accountable, Consulted, Informed
RCM	Risk & Control Matrix
RCSA	Risk & Control Self Assessment
RFI	Request For Information
RFP	Request For Proposal
SaaS	Software as a Service
SANS	SysAdmin, Audit, Network & Security
SASE	Secure Access Service Edge
SATAN	Security Administrator Tool for Analyzing Networks
SDLC	Software Development LifeCycle
SIC	Security Identification Code
SIEM	Security Incident & Event Management

Acronym	Expansion
SIRT	Security Incident Response Ticket
SOC	System and Organization Controls
SPOF	Single Point Of Failure
SQL	Structured Query Language
SSAE	Statement on Standards for Attestation Engagements
SSDLC	Secure Software Development LifeCycle
SSO	Single Sign On
STIX	Structured Threat Information Expression
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TTOE	Technical Target Of Evaluation
TTPs	Tactics, Techniques, & Procedures
TTR	Time To Respond
UBA	User Behavioral Analysis
URL	Universal Resource Locator
VPN	Virtual Private Network
WAFW	Web Application Firewall
ZTA	Zero Trust Architecture