Cybersecurity Risk Assessment

Ayob Sether

Independent Researcher

April 2026

Author Note

Ayob Sether https://orcid.org/0000-0002-1578-6224

Table of Contents

Abstract

This study presents cybersecurity risk assessment addressing growing national cybersecurity, economic, and societal risks of modern cyber threats. Cybersecurity has evolved into a strategic national imperative, where cyber incidents can disrupt essential services, degrade military capabilities, and trigger cascading failures across critical infrastructure. Cyber operations increasingly target military hardware and defense systems, including aircraft, fighter jet platforms, and drone and missile navigation through GPS spoofing and jamming. Intrusions into defense contractors further expose sensitive operational data, demonstrating that cyber warfare impacts both civilian and military domains without physical engagement.

This evolving landscape confirms cybersecurity as a core national cybersecurity priority, where failure to manage, risks can lead to economic instability, military vulnerability, societal disruption, and far-reaching geopolitical consequences, ultimately threatening national stability and existence.

The framework adopts a governance-driven approach aligned with ISO/IEC 27001, introducing a quantitative risk model. Using telecommunications as a primary case study due to its cross-sector dependencies, the framework supports practical tools such as risk assessment templates, asset registers, and sector dashboards, emphasizing the need to extend cybersecurity beyond Information Technology (IT) into national governance and resilience strategies.

Keywords: cybersecurity risk assessment, governance, compliance, ISO/IEC 27001, quantitative risk model

Cybersecurity Risk Assessment

Cybersecurity

Before discussing cybersecurity, it is essential to recognize its critical national importance. In the modern era, warfare has evolved beyond traditional battlefields; what is often referred to as “fifth-generation warfare” is increasingly fought in the cyber domain, where attacks target a nation’s digital infrastructure, economy, military capability, and public trust rather than its physical borders. A single cyber incident can disrupt power grids, paralyze financial systems, shut down telecommunications, and expose millions of citizens’ data without a single shot being fired (Saleem et al., 2026; Ramage et al., 2025). For instance, the Stuxnet cyberattack demonstrated how malware could physically damage critical infrastructure (Cybersecurity & Infrastructure Security Agency, 2014); the Colonial Pipeline ransomware attack caused fuel shortages across the United States (INSURICA Insurance Management Network, 2024); and the Ukraine power grid cyberattack showed how cyber operations can directly impact national energy systems (Humphreys, 2024).

More critically, cyber operations have increasingly targeted military hardware and defense systems. For instance, researchers demonstrated remote exploitation of aircraft systems in a Boeing 757 cybersecurity test (Paganini, 2017). Vulnerabilities have been identified in advanced fighter jet platforms like the F-35 Lightning II related to software and logistics systems (Burgess, 2015). GPS spoofing and jamming incidents have affected navigation of military drones and missiles, highlighting risks to precision guided weapons (SKYbrary Aviation Safety, n.d.). Additionally, cyber intrusions into defense contractors such as Lockheed Martin have raised concerns about exposure of sensitive weapons system data (British Broadcasting Corporation, 2011). These examples demonstrate that modern cyber warfare can influence not

only civilian critical infrastructure but also missiles, aircraft, and critical defense hardware, potentially degrading combat capability without direct kinetic engagement.

This evolving threat landscape proves that cybersecurity is no longer just an Information Technology (IT) concern. It is a core national security priority, where failure to manage, cyber risks can lead to economic instability, military vulnerability, societal disruption, and far-reaching geopolitical consequences, ultimately escalating into a direct threat to a nation's survival and existence (Basak, 2024; Cobos et al., 2024).

Cybersecurity Risk

As threat landscapes evolve, cybersecurity threats continue to expand in complexity and scope. These threats can be broadly categorized into several types. For instance, GPS spoofing and jamming, critical infrastructure attacks, regulatory compliance gaps, malware attacks, social engineering exploits, insider threats, Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS), ransomware, Man-in-the-Middle (MitM) attacks and, Supply chain attacks (Moore, n.d.).

The Cybersecurity and Infrastructure Security Agency (CISA) emphasizes that cybersecurity threats pose a significant risk to critical infrastructure assets sectors including but not limited to telecommunications, financial services, healthcare, cloud services, military hardware and defense systems (Cybersecurity & Infrastructure Security Agency, n.d.).

The increasing reliance on cloud computing and data-driven systems across the world further elevates the importance of cybersecurity risk. Cloud environments introduce shared responsibility models, complex supply chains, and evolving threat vectors that require continuous, independent risk evaluation. National Institute of Standards and Technology (NIST)

underscores the importance of managing cybersecurity risks in cloud environments through structured risk management and continuous assessment (Bohn Robert et al., 2020).

Cybersecurity Ventures projected that global cybercrime costs reach $10.5 trillion annually by 2025, making cybercrime one of the largest economic threats worldwide (Morgan & Sausalito, 2020).

International Business Machines (IBM)'s cost of a data breach report indicates that data breaches result in significant financial losses, operational disruption, and reputational harm for affected organizations (International Business Machines, 2025).

The U.S. Department of Homeland Security identifies cybersecurity attacks on critical infrastructure assets as a major national security concern due to their potential to disrupt essential services (The White House, 2013).

The World Economic Forum ranks cybersecurity risks among the top global risks affecting economic stability and national resilience (Zahidi et al., 2024).

At the policy level, cybersecurity is recognized as a strategic priority affecting economic security, consumer protection, and public trust. The U.S. White House National Cybersecurity Strategy emphasizes risk-based approaches, public private collaboration, and accountability as pillars of national cybersecurity resilience (Shankar, 2024).

Identifying the Critical Need

The authoritative reports cited above do more than establish the general importance of cybersecurity: they reveal a specific and urgent national vulnerability; the governance and assurance gap in complex, interconnected systems (National Institute of Standards and Technology, 2018a).

The Gap

While technical safeguards are essential, agencies like NIST, CISA, and the U.S. Government Accountability Office (GAO) consistently emphasize that resilience depends on objective, standards-based risk assessment and governance (National Institute of Standards and Technology, 2018b).

The (GAO) has repeatedly identified information security as a high-risk area for the federal government, highlighting the need for assessments to address persistent cybersecurity weaknesses (U.S. Government Accountability Office, 2025).

Why Cybersecurity Risk Assessment is Essential?

The NIST states that cybersecurity risk management is essential to protecting critical infrastructure assets. The ISO/IEC 27001 and NIST Cybersecurity Framework are widely adopted across public and private sectors to manage and reduce cybersecurity risk (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022).

Cybersecurity threats can result in significant data breaches, operational disruptions, financial losses, exposing sensitive information, violating privacy. Cybersecurity threats can also result in triggering lawsuits, imposing heavy regulatory fines, and permanently damaging reputation, sometimes overnight (Hussain Seh et al., 2020). Yet cybersecurity is still treated as an IT-only responsibility, focusing on systems, firewalls, encryption, and access controls, while overlooking the weakest link — the broader organizational ecosystem, including people, processes, and third-party dependencies (Information Systems Audit and Control Association, 2010). Cybersecurity risks do not live only in networks; they exist across the entire organization, and when risk assessments are performed solely within IT, they create a narrow and often biased

view that fails to capture real impact. Knowing a threat exists is not enough — if it is not understood where the risk is, how likely it is to occur, and how severe its impact could be, the organization is already exposed. Worse, organizations may overinvest in low impact risks or underestimate high impact ones, leading either to wasted resources or catastrophic loss (National Institute of Standards and Technology, 2012). This is why cybersecurity risk assessment must extend beyond IT and be conducted by independent experts or autonomous functions that provide an unbiased, enterprise-wide perspective, clearly identifying where risks exist, how likely they are, and what their true impact will be, enabling organizations to act before damage occurs. Because in cybersecurity, the greatest danger is not what one knows, but what one fails to see coming (Mulugeta Melaku, 2023).

Cybersecurity Risk Assessment Operational Framework

Objective

Build operational credibility in cybersecurity risk assessment and critical infrastructure resilience across multiple sectors. The focus should be on developing framework that emphasizes practical risk assessment tools and engagement, demonstrating measurable value (Aghazadeh Ardebili, 2024).

Critical Infrastructure Qualification Model

Develop a practical *Critical Infrastructure Cybersecurity Risk Quantification Model* that enables structured evaluation of cybersecurity risks affecting national critical infrastructure assets. The model should support cross-sector comparison of cybersecurity risks and resilience capabilities (Khaki Kaleba & Tembo, 2025).

Critical Infrastructure Assets Sectors

The operational framework should be applicable to all critical infrastructure assets sectors that support national economic stability and public services. The initial sectors recommended for cybersecurity risk assessment should be, including but not limited to (National Institute of Standards and Technology, 2012);

- Telecommunications
- Banking and Financial Services
- Digital Infrastructure and Data Centers
- Government Digital Services
- Energy (Electricity, Oil & Gas)
- Transportation (Aviation, Rail and Maritime)
- Healthcare Systems
- Water and Utilities
- Military & Defense
- Cross-Sector Assets (Important for All Sectors)

Cybersecurity Impact

Cybersecurity Impact is the effect of a cybersecurity incident on the Confidentiality, Integrity, and Availability of systems and data, potentially causing service disruption, data loss, financial damage, and broader impacts on users and critical infrastructure assets (Tripathi, 2025).

Service Availability Impact

Services unavailable due to a cybersecurity incident, for instance national telecom network unavailable for hours and banking payment system offline for hours. Measured metrics for instance (Organization for Economic Co-operation and Development, 2022);

- Service downtime
- Number of critical systems offline
- Recovery time – Mean Time to Recovery ((MTTR)

Confidentiality Impact

Unauthorized exposure of sensitive data, for instance millions of customer records leaked and Government citizen database breached. Measured metrics for instance (United Nations Children's Fund, n.d.);

- Number of records exposed
- Data classification affected (public, confidential and classified)
- Number of users whose personal data was compromised
- Percentage of critical datasets exposed

Data Integrity Impact

Unauthorized modification or corruption of data or systems, for instance manipulated bank transaction records and altered Supervisory Control And Data Acquisition (SCADA) sensor readings. Measured metrics for instance (Dotter et al., 2025);

- Number of systems compromised
- Number of altered transactions
- Data corruption percentage
- Operational decision errors caused by data manipulation

Connectivity and Network Impact

Disruption of network communications and connectivity, for instance Border Gateway Protocol (BGP) hijacking causing global routing disruption and Telecom backbone outage. Measured metrics for instance (European Union Agency for Cybersecurity, 2024);

- Network throughput degradation
- Number of network nodes affected
- Percentage of internet traffic disrupted
- Loss of connectivity to international networks

Users and Customers Impact

People or organizations impacted, for instance millions of mobile subscribers unable to access services. Measured metrics for instance (Zurich Insurance Group, 2025);

- Number of users affected
- Percentage of total users impacted
- Number of organizations impacted
- Number of critical infrastructure operators affected

Economic Impact

Financial damage caused by the cyber incident, for instance manufacturing shutdown costing billions. Measured metrics for instance (Cobos & Cakir, 2024);

- Direct financial losses
- Operational recovery cost
- Revenue loss due to service disruption
- Supply chain losses
- Insurance claims

Cascading Effects (Cross-Sector) Impact

Secondary impacts on interconnected sectors, for instance, Telecom outage disrupting banking, hospitals, and government services. Measured metrics for instance (Toregas & Santos, 2019);

- Number of dependent sectors affected
- Duration of cascading disruption
- Number of downstream organizations impacted
- Supply chain disruption level

National Security Impact

Impact on national stability or security systems, for instance power grid attack affecting multiple regions. Measured metrics for instance (Consultants to Government & Industries, 2013);

- Disruption of national defense communications
- Impact on emergency services
- Critical infrastructure failure
- Strategic geopolitical impact

Public Safety Impact

Risk to human life or public safety. Measured metrics for instance (Aldosari, 2025);

- Hospitals unable to provide emergency care
- Transportation accidents due to system outages
- Industrial safety failures

Reputational and Trust Impact

Loss of trust among customers, citizens, or stakeholders (Nawaz Khan et al., 2025). Measured for instance;

- Customer churn rate
- Brand value decline
- Stock price impact
- Public confidence index

Sector Wide Critical Infrastructure Assets

Critical infrastructure assets for each sector including but not limited to:

Telecommunications

Critical infrastructure assets in telecommunications sector, for instance (Jijo George et al., 2015);

- Core network infrastructure (MSC, HLR/HSS, IMS)
- 4G/5G core network systems
- Backbone routers (Internet)
- International gateways
- Radio access networks and base stations
- Network management systems
- Telecom data centers
- Supply Chain

Banking and Financial Services Sector

Critical infrastructure assets in banking and financial services sector, for instance (Othihiwa et al., 2025);

- Core banking systems
- Payment processing systems
- Interbank transfer systems (RTGS / national payment networks)
- ATM networks and ATM switch infrastructure
- Online banking platforms (internet banking)
- Mobile banking platforms
- Card payment processing systems (POS networks)
- Financial market trading platforms
- Central securities depository systems
- Clearing and settlement systems
- Fraud detection and transaction monitoring systems
- Banking data centers
- Customer identity and authentication systems
- Financial messaging infrastructure (SWIFT network connectivity)
- Banking supply chain (payment processors, fintech integrations, third-party service providers)

Digital Infrastructure and Data Centers

Critical infrastructure assets in digital infrastructure and data centers sector support cloud services, Internet hosting, digital platforms, and national IT infrastructure, for instance (Mell & Grance, 2011);

- Hyperscale data center facilities
- Colocation data centers
- Cloud infrastructure platforms (IaaS/PaaS)
- Internet Exchange Points (IXPs)
- Data center network switching infrastructure
- Storage systems and storage area networks (SAN)
- Virtualization platforms (VMware & Hyper-V)
- Container orchestration platforms (Kubernetes clusters)
- Identity and access management infrastructure
- Backup and disaster recovery systems
- Content delivery networks (CDN)
- Physical infrastructure (power systems, cooling systems, fire suppression)
- Data center security systems (access control, CCTV, environmental monitoring)
- Software-defined networking (SDN) infrastructure
- Third-party cloud service provider integrations

Government Digital Services

Critical infrastructure assets in government digital services sector enable public administration, citizen services, and national governance platforms, for instance (Organisation for Economic Co-operation and Development, 2024);

- National digital identity systems
- Government service portals (e-government platforms)
- National population registry databases
- Taxation and revenue management systems

- Immigration and border control systems
- National cybersecurity monitoring systems
- Government cloud infrastructure
- Public service payment systems
- Document management and records systems
- Government email and communication platforms
- National election infrastructure systems
- National law enforcement databases
- Government network infrastructure
- Public sector data centers
- Interagency data exchange platforms

Energy Sector (Electricity, Oil & Gas)

Critical infrastructure assets in energy sector (Electricity, Oil & Gas) are among the most critical national infrastructure due to its impact on economic stability and public safety, for instance (Kreso, 2025);

- Power generation control systems
- Electrical grid control systems (SCADA/ICS)
- Energy transmission systems
- Power distribution networks
- Substation automation systems
- Energy Management Systems (EMS)
- Oil and gas pipeline monitoring systems
- Oil refinery control systems

- Liquefied Natural Gas (LNG) facilities
- Smart grid infrastructure
- Industrial Control Systems (ICS)
- Supervisory Control And Data Acquisition (SCADA) systems
- Energy trading platforms
- Remote Terminal Units (RTUs)
- Energy sector data centers

Transportation (Aviation, Rail & Maritime)

Critical infrastructure assets in transportation (Aviation, Rail & Maritime) support national mobility, trade, and logistics, for instance (DOĞAN, 2023; Lo & Bouarfa, 2021);

Aviation

- Air traffic management systems
- Airport operational control systems
- Flight information systems
- Aviation navigation systems
- Airport security systems

Rail

- Railway signaling systems
- Train control and monitoring systems
- Rail traffic management systems
- Railway communication systems

Maritime

- Port management systems

- Vessel traffic management systems
- Maritime navigation systems
- Cargo logistics platforms
- Cross-sector transportation systems
- Transportation control centers
- Ticketing and reservation systems

Healthcare Systems

Critical infrastructure assets in healthcare systems supports public health and emergency medical services, for instance (Liveri et al., 2015);

- Hospital Information Systems (HIS)
- Electronic Health Record (EHR) systems
- Medical imaging e.g. Picture Archiving and Communication System (PACS)
- Laboratory information systems
- Telemedicine platforms
- Medical device networks
- Hospital network infrastructure
- Emergency response systems
- Pharmaceutical supply chain systems
- Healthcare data centers
- Clinical decision support systems
- Medical research databases
- National health insurance systems
- Hospital building management systems

- Patient monitoring systems

Water and Utilities

Critical infrastructure assets in water and utilities ensures public health, sanitation, and essential services, for instance (Kumar Balaraman et al., 2025; Halliday, 2003);

- Water treatment plant control systems
- Water distribution network control systems
- Water quality monitoring systems
- Wastewater treatment control systems
- Pumping station automation systems
- Reservoir monitoring systems
- Industrial control systems for water plants
- Supervisory Control And Data Acquisition (SCADA) systems
- Smart water meter infrastructure
- Utility network management systems
- Emergency water supply systems
- Water sector data centers
- Environmental monitoring systems
- Utility billing and management systems
- Remote telemetry units for water systems

Military & Defense

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), for instance (Ross et al., 2021; U. S. Office of the Under Secretary of Defense for Policy, 2016; U. S. Government Accountability Office, 2009);

- National military command centers
- Strategic command & control systems
- Battlefield management systems
- Military communication networks (secure voice/data)
- Satellite communication systems
- Intelligence processing systems

Impact; Loss of command authority and miscommunication in combat.

Weapons systems (Missiles & Strategic Weapons), for instance;

- Missile guidance and control systems
- Air defense systems (e.g., radar-guided systems)
- Fire control systems
- Precision-guided weapon systems
- Nuclear command and control systems

Impact; Misfire, failure to launch and unauthorized activation.

Military aircraft & Unmanned Aerial Vehicle (UAV) systems, for instance;

- Avionics systems (navigation & targeting)
- Flight control software
- UAV/drone control systems
- Ground control stations

- Aircraft mission planning systems

Impact; Loss of aircraft control and mission failure.

Naval systems & maritime defense, for instance;

- Warship combat management systems
- Submarine control systems
- Naval radar and sonar systems
- Ship navigation systems (GPS & INS)

Impact; Navigation failure and combat system compromise.

Military satellites & space systems, for instance;

- GPS/navigation satellite systems
- Surveillance and reconnaissance satellites
- Satellite ground control stations
- Missile early warning systems

Impact; Loss of navigation and blind defense systems.

Defense & military cyber and IT infrastructure, for instance;

- Military data centers
- Cybersecurity Operation Centers (SOC)
- Defense networks and cloud systems
- Encryption and cryptographic systems

Impact; Data breach and operational paralysis.

Logistics & supply chain systems, for instance;

- Military logistics management systems
- Ammunition supply systems

- Fuel supply systems
- Defense procurement platforms

Impact; Supply disruption and mission failure.

Defense Industrial Base (DIB), for instance;

- Defense contractors (weapons manufacturers)
- R&D facilities
- Military technology development systems
- Software development environments

Impact; Intellectual property theft and weakened defense capability.

Training & simulation systems, for instance;

- Flight simulators
- War gaming platforms
- Training command systems

Impact; Reduced readiness and incorrect training outcomes.

Critical facilities & physical infrastructure, for instance;

- Military bases and installations
- Airbases and runways
- Missile silos
- Secure bunkers and command facilities

Impact; Physical and operational disruption.

Cross-Sector Assets (Important for All Sectors)

Some critical infrastructure assets components are common across many sectors, for instance (National Institute of Standards and Technology, 2024; Boyens et al., 2022);

- Data centers
- Cloud infrastructure
- Identity and access management systems
- Network infrastructure
- Operational Technology (OT) control systems
- Cybersecurity monitoring systems
- Supply chain and vendor systems
- Backup and disaster recovery systems

Cybersecurity Risk Assessment for Telecommunications Sector

Telecommunications Sector Overview

In this study, the focus is limited to the telecommunications sector, as a comprehensive analysis of all critical infrastructure assets sectors is beyond the scope of this study. However, the same approach, methodology, and principles presented here are equally applicable across other sectors e.g., Banking and Financial Services, Digital Infrastructure and Data Centers, as well as all other critical infrastructure assets sectors, enabling a broader extension of this framework. The telecommunications sector forms the backbone of national digital infrastructure. Telecom networks enable banking, government services, energy systems, transportation, defense communications, and Internet connectivity. Cybersecurity incidents affecting telecom infrastructure may therefore cause cascading disruptions across multiple sectors. Operational cybersecurity efforts must therefore prioritize resilience of telecom critical infrastructure assets (Sadiku et al., 2024; Reddy Palleti et al., 2021).

Telecommunications Qualification Model

The goal is to develop a practical *Telecommunications Cybersecurity Risk Quantification Model* based on ISO/IEC 27001 that enables structured evaluation of cybersecurity risks affecting telecom critical infrastructure assets. This model will allow telecommunications operators and regulators to quantify cybersecurity risk exposure and identify systemic vulnerabilities (Ali Siddiqui ET AL., 2025; Patchamatla, 2014).

Number of Subscribers Affected

It measures how many mobile, Internet, or telecom users lose service or are impacted during a cybersecurity incident. For instance, the Rogers Communications outage 2022 affected over 12 million subscribers, disrupting mobile, Internet, and payment systems across Canada (Xona Partners Inc, 2023a).

Impact Insight;

- Direct measure of population impact
- Used to assess severity level (local vs national)

Geographic Coverage Disruption

It measures the physical area (cities, regions, or nationwide) affected by telecom service disruption. For instance, the Rogers Communications outage caused nationwide disruption across Canada, affecting multiple provinces simultaneously (Xona Partners Inc, 2023b).

Impact Insight;

- Local outage → limited impact
- Nationwide outage → critical national impact

Emergency Service Availability

It measures whether emergency communication systems (emergency services, police and/or ambulance) remain operational. For instance, during the Rogers Communications outage, 911 emergency services were disrupted, preventing citizens from reaching emergency responders (Xona Partners Inc, 2023c).

Impact Insight;

- Direct link to public safety and life risk
- Considered critical severity indicator

Internet Backbone Connectivity Impact

It measures disruption to core Internet infrastructure, including backbone routers, IXPs, and international connectivity. For instance, the Facebook outage 2021 was caused by BGP routing issue, effectively disconnecting Facebook's global infrastructure from the Internet (Janardhan, 2021).

Impact Insight;

- Affects global connectivity
- Can isolate entire networks or countries

Cascading Effects on Banking and Government Services

It measures how telecom disruption impacts dependent sectors such as banking, ATMs, payments, and government systems. For instance, during the Rogers Communications outage Bank ATMs stopped working, payment systems failed and government services were inaccessible (Saropa Contacts News, 2025).

Impact Insight;

- Demonstrates interdependency risk

- Telecom failure → multi-sector national disruption

Sector Threat Landscape

Cybersecurity threats affecting critical infrastructure assets may include but not limited to (Donegan, (2021; Boas et al., n.d.);

- Nation state cyber espionage
- Distributed Denial of Service (DDoS) attacks
- BGP route hijacking
- SS7/Diameter signaling exploitation
- Ransomware targeting operational systems
- Supply chain compromise
- Insider threats
- Industrial control system attacks
- Data exfiltration operations

Cybersecurity Risk Assessment Operational Tools

Standards based cybersecurity frameworks are critical tools for managing cybersecurity risk at a national-level. ISO/IEC 27001 is recognized globally as a leading standard for Information security, cybersecurity and privacy protection — Information security management systems and is widely adopted to meet regulatory and compliance requirements (International Organization for Standardization, 2022).

Risk Assessment Strategy Handbook ISO/IEC 27001

A comprehensive handbook should be developed that serves as a practical reference for all controls and themes of ISO/IEC 27001, detailing their requirements for assessment,

implementation, and testing. For instance, within People Controls (Theme) of ISO/IEC 27001:2022, the handbook outlines each specific control along with clear guidance on what needs to be evaluated, how it should be tested, and the evidence required to demonstrate compliance. For instance, “People Controls” (Theme) of ISO/IEC 27001:2022 requires following controls (International Organization for Standardization, 2022);

- 6.3 Information security awareness, education and training
- 6.4 Disciplinary process
- 6.5 Responsibilities after termination or change of employment
- 6.6 Confidentiality or non-disclosure agreements
- 6.7 Remote working
- 6.8 Information security event reporting

It further provides structured insights into how each control supports risk assessment and risk treatment objectives, ensuring organizations can consistently and effectively satisfy the standard’s requirements (International Organization for Standardization, 2022).

Similarly, a comprehensive set of operational cybersecurity risk assessment tools can be developed, including risk assessment questionnaires, structured assessment forms, asset classification registers, sector-wise critical infrastructure assets risk dashboards, and incident impact scoring templatesç These tools enable organizations to systematically identify, evaluate, and quantify risks, while providing standardized, repeatable, and data-driven approaches to support effective decision-making, risk prioritization, and continuous monitoring across critical infrastructure assets sectors (Bresnahan, n.d.).

Scoring Model Variables

The cybersecurity risk scoring model should incorporate, for instance (Zadeh et al., 2023);

- Likelihood of cybersecurity attack (1–5)
- Impact severity (1–5)
- Infrastructure interdependency factor (1–2)
- Security maturity reduction value (0–25)
- Service disruption duration
- Population or customer impact
- Cross-sector dependency impact

Risk Level Formula

Equation (1): Risk Level = (Likelihood × Impact × Interdependency Factor) - Security Maturity Reduction Value. The final risk level should be normalized within a defined risk range and mapped to risk levels such as following (Yoo & Han-Seon, 2021; Sheehan et al., 2021);

- Very Low
- Low
- Medium
- High
- Critical

Risk Level Calculation Method 0–50 Scale

This 0–50 scale works well because most matrices produce scores between 0–50. There are 3 steps to calculate Risk Level of any asset category (Emma, 2024; Nurthen, 2023);

- Calculate security maturity reduction value first

- Then calculate raw risk for asset category
- And then use security maturity reduction value to calculate risk level for that asset category

Risk Matrix

Following are variables of scoring model, also as shown in Table 1 (Emma, 2024; Nurthen, 2023);

- Likelihood of attack
- Impact severity
- Infrastructure interdependency
- Security maturity level
- Subscriber impact
- Cross-sector dependency impact

Assets Categories of Telecommunications Sector

For instance (Jijo George et al., 2015);

- Core network infrastructure (MSC, HLR/HSS, IMS)
- 4G/5G core network systems
- Backbone routers (Internet)
- International gateways
- Radio access networks and base stations
- Network management systems
- Telecom data centers
- Supply chain

Security Domains of Each Asset Category of Telecommunications Sector

For instance, below are security domains of asset category core network infrastructure (MSC, HLR/HSS, IMS), same security domains can be applied to all other assets categories (International Organization for Standardization, 2022);

- Governance & policy
- Asset management
- Network security
- Identity & access management
- Threat detection & monitoring
- Incident response
- Vulnerability management
- Third party security
- Backup & resilience

Score Each Security Domain (1–5)

Security domain for instance, governance policy, asset management, network security, identity & access management and threat detection & monıtorıng, as shown ın Table 2.

Control Score

Control score for instance, no formal controls, basic controls exist, documented processes, managed & monitored and continuous improvement, as shown in Table 3.

Maturity Level to Security Maturity Reduction Value

Maturity level for instance, level 1 with Security Maturity Reduction Value initial = 0, level 2 with Security Maturity Reduction Value managed = 5, level 3 with Security Maturity

Reduction Value defined = 10, level 4 with Security Maturity Reduction Value managed = 15, level 5 with Security Maturity Reduction Value advanced = 20, level 6 with Security Maturity Reduction Value optimized = 25, as shown in Table 4 (Saudi Arabian Monetary Authority, 2017).

Calculate Security Maturity Reduction Value

For instance; Equation (2): Security Maturity Reduction Value = (Add All Security Control Domains) / (Number of Security Control Domains). As shown in Table 2, Security Maturity Reduction Value = (4+2+4+3+5+4+3+4) / 8 = 3.625 is rounded up to the nearest whole number 4 = Level 4 and Level 4, as shown in Table 4, is Managed = 15. Therefore, Security Maturity Reduction Value = 15. Security Maturity Reduction Value (0–25) is a risk adjustment factor used in quantitative cybersecurity risk models. It reduces the raw risk score based on how mature and effective an organization's cybersecurity controls are. For instance (Saudi Arabian Monetary Authority, 2017; Bistarelli et al., S., n.d.);

- If Security Maturity Reduction Value is low, reduction is small → risk increases
- If Security Maturity Reduction Value is high, reduction is large → risk decreases

This prevents overestimating risk when strong controls already exist.

Why Security Maturity Reduction Value is Used?

Traditional risk matrices use only following;

- Likelihood
- Impact

But strength of security controls is ignored. For instance, if the system already has following;

- 24/7 SOC monitoring

- Zero Trust architecture
- Network segmentation
- Threat intelligence integration

Then the actual operational risk is lower (reduction) and that reduction is represented by Security Maturity Reduction Value (Saudi Arabian Monetary Authority, 2017; Bistarelli et al., S., n.d.). This 0–50 range works well because most matrices produce scores between 0–50.

Evidence Used to Score Security Maturity Reduction Value

For instance, when assessing maturity, verify (Bernardo et al.,2025; National Institute of Standards and Technology, 2024);

Governance

- Cybersecurity policy
- Risk management framework
- Board oversight

Technical Controls

- Network segmentation
- MFA deployment
- Zero Trust architecture

Monitoring

- SOC capability
- SIEM
- Threat intelligence feeds

Response

- Incident response playbooks

- Tabletop exercises
- Recovery procedures

When Security Maturity Should Not Reduce Risk?

For instance, do not reduce risk if (de Lima et al., 2024; Myung Song et al., 2024);

- Controls exist but are not enforced
- Monitoring exists but alerts ignored
- Policies exist but not implemented
- Third-party risk unmanaged

Only effective controls justify reduction.

Best Practice for Risk Models of Telecommunications Sector

For national critical infrastructure assets cybersecurity risk assessments;

Security Maturity Reduction = (minimum maturity score across critical domains).

Calculate Raw Risk for Assets Categories of Telecommunications Sector

First, calculate one-by-one Raw Risk of all asset categories. For instance, asset category Core network infrastructure (MSC, HLR/HSS, IMS) (Pinzariu & Anagnostakis, 2022; Evrin, (2021; Tatar et al., 2020);

- Likelihood = 4
- Impact = 5
- Interdependency = 2

Equation (3): Raw risk = (Likelihood × Impact × Interdependency) = 4x5x2 = 40. In this example, asset category core network infrastructure (MSC, HLR/HSS, IMS) Raw Risk is 40.

Calculate Risk Level for Assets Categories of Telecommunications Sector

After calculating Raw Risk, calculate Risk Level of each asset category. For instance, Risk level = Raw risk – Security Maturity Reduction Value = 40 - 15 = 25. As shown in Table 5, the Risk Level = 25 is Medium level for asset category core network infrastructure (MSC, HLR/HSS, IMS). Cybersecurity risk management should focus on Risk Level rather than Raw Risk (Pinzariu & Anagnostakis, 2022; Evrin, (2021; Tatar et al., 2020).

Risk Level 0-50 Scale for Telecommunications Sector

Risk level for instance, 0-5 very low, 6-15 low, 16-25 medium, 26-40 high and 41-50 critical, as shown in Table 5.

Important Calculation Note

Negative values should be normalized to 0. For instance, Risk Level = (Likelihood 1 x Impact 1 x Interdependency 1) - Security Maturity Reduction Value 25 i.e. Risk Level = (1 x 1 x 1) - 25 = -24 ~ 0. Therefore, in this example, Risk Level = 0 which is Very Low, as shown in Table 5.

Conclusion and Future Study

This study establishes a structured cybersecurity risk assessment that addresses the growing complexity and scale of cyber threats impacting critical infrastructure and national security. It demonstrates that cybersecurity risk is no longer confined to technical domains but represents a strategic challenge requiring governance-driven, cross-sector, and data-driven approaches. The proposed quantitative risk model, incorporating likelihood, impact, interdependency, and security maturity, enables more accurate and practical assessment of real-world cyber risks while supporting informed decision-making and prioritization (Gilbert & Abiola Gilbert, 2024; National Institute of Standards and Technology, 2018).

By applying the framework to the telecommunications sector, this study highlights the significance of interdependencies across critical infrastructure sectors and the potential for cascading impacts. The development of operational tools such as risk assessment templates, asset registers, and sector dashboards further strengthens the ability of organizations and governments to implement consistent, scalable, and repeatable cybersecurity risk management practices. Ultimately, the framework reinforces the need to elevate cybersecurity from an IT function to a national governance priority to enhance resilience, protect critical infrastructure, and mitigate systemic cyber risks (Sadiku et al., 2024; Reddy Palleti et al., 2021).

Future research should focus on expanding this operational framework into a comprehensive national-level cybersecurity governance architecture. This includes transforming the model into a national cybersecurity risk governance architecture, incorporating cross-ministry and departments coordination mechanisms, and establishing

unified governance structures across critical sectors. Additionally, the development of a National Cybersecurity Risk Maturity Index will enable benchmarking and continuous improvement of sectoral resilience (National Institute of Standards and Technology, 2018).

Further studies should map interdependencies across sectors to better understand cascading risks and systemic vulnerabilities. A strategic priority should also be the formulation of national cybersecurity roadmap, outlining clear objectives, policy directions, and implementation strategies. These advancements will support the evolution from operational risk assessment to strategic national cybersecurity governance, strengthening long-term resilience and national security (Shukla et al., 2025; Petit et al., 2015).

References

Aghazadeh Ardebili, A., Lezzi, M. & Pourmadadkar, M. (2024, 17 December 17). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. https://www.mdpi.com/2076-3417/14/24/11807

Aldosari, B. (2025, May 6). Cybersecurity in Healthcare: New Threat to Patient Safety. https://pmc.ncbi.nlm.nih.gov/articles/PMC12141808

Ali Siddiqui, S., Thapa, C., Wang, D., Holland, R., Shao, W., Camtepe, S., Suzuki, H., & Shah, R. (2025, July 9). TELSAFE: Security Gap Quantitative Risk Assessment Framework. https://arxiv.org/abs/2507.06497

Basak, B. (2024, April 15). The Impact of Cybersecurity Threats on National Security: Strategies. https://ijhssm.org/issue_dcp/The%20Impact%20of%20Cybersecurity%20Threats%20on%20National%20Security%20%20Strategies.pdf

Bernardo, L., Malta, S. & Magalhães, J. (2025, March 28). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. https://www.mdpi.com/2079-9292/14/7/1364

Bistarelli, S., Geoli, S., Luchini, G & Mercanti, I. (n.d.). Analysis and Study of a Cybersecurity Maturity Assessment System for SMEs. https://ceur-ws.org/Vol-3962/paper27.pdf

Boas, E. C. V., De Vito, I. F., Domiciano, A. C. & Aquino, G. P. (n.d.). Cybersecurity in Fixed Broadband Networks. https://inatel.br/cxsc/documents/cybersecurity-in-fixed-broadband-networks.pdf

Bohn Robert B., Lee Craig A. & Martial, M. (2020, February). The NIST Cloud Federation Reference Architecture. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-332.pdf

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. & Fallon, M. (2022, May). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

Bresnahan, E. (n.d.). 3 Templates for a Comprehensive Cybersecurity Risk Assessment. https://www.cybersaint.io/blog/cyber-security-risk-assessment-templates

British Broadcasting Corporation. (2011, May 30). US defence firm Lockheed Martin hit by cyber-attack. BBC. https://www.bbc.com/news/world-us-canada-13587785

Burgess, A. (2015, December 16). F-35 cyber security testing delay prompts vulnerability concerns. https://www.themanufacturer.com/articles/f-35-cyber-security-testing-delay-prompts-vulnerability-concerns

Cobos, E.V. & Cakir, S. (2024). A Review of the Economic Costs of Cyber Incidents. https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf

Cobos, E. V., Cakir, S., Mei-Zahav, H. & Berkay Barakcin, B. (2024). The Role of Cybersecurity in Economic Performance. http://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf

Consultants to Government & Industries. (2013, April 10). Developing a Framework to Improve Critical Infrastructure Cybersecurity. https://verifiedvoting.org/developing-a-framework-to-improve-critical-infrastructure-cybersecurity/

Cybersecurity & Infrastructure Security Agency. (n.d.). Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cybersecurity & Infrastructure Security Agency. (2014, January 08). Stuxnet Malware Mitigation (Update B). https://www.cisa.gov/news-events/ics-advisories/icsa-10-238-01b

de Lima, M., da Cruz, G. Jr., da Cunha, D. & Barreto, J. P. S. (2024, December 10). A Flexible Framework for Evaluating Cyber Security Maturity and Risks in Electric Power Generation Organizations. https://dl.acm.org/doi/full/10.1145/3697090.3700482

DOĞAN, D. (2023, October). MARITIME CRITICAL INFRASTRUCTURE PROTECTION (MCIP) IN A CHANGING SECURITY ENVIRONMENT. https://www.marseccoe.org/wp-content/uploads/2023/10/Maritime-Critical-Infrastructure-Protection-.pdf

Donegan, P. (2021, January). Learnings from Real World Telco Security Incidents. https://www.a10networks.com/wp-content/uploads/A10-WP-Lessons-from-Real-World-Telco-Security-Incidents.pdf

Dotter, M., Garris, M., Khemani, I., Bronwyn, P., Schiro, N., Nethery Snyder, J. & Mohammad, Z. (2025, December). Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile). https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8596.iprd.pdf

Emma. (2024, November 28). How To Use (And Understand) A 5x5 Risk Matrix. https://www.haspod.com/blog/paperwork/5x5-risk-matrix

European Union Agency for Cybersecurity. (2024, December). 2024 Report on the State of Cybersecurity In the Union. https://www.enisa.europa.eu/sites/default/files/2024-

11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

Evrin, V. (2021, April 28). Risk Assessment and Analysis Methods: Qualitative and Quantitative. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

Gilbert, C. & Abiola Gilbert, M. (2024, December). Cybersecurity Risk Management Frameworks for Critical Infrastructure Protection. https://www.researchgate.net/publication/386381194_Cybersecurity_Risk_Management_Frameworks_for_Critical_Infrastructure_Protection

Halliday, R. A. (2003). Water, Critical Infrastructure Protection and Emergency Management. https://publications.gc.ca/collections/collection_2008/ps-sp/PS4-7-2004E.pdf

Humphreys, B. E. ((2024, May 17). Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience. https://www.congress.gov/crs-product/R48067

Hussain Seh, A., Mohammad, Z., Mamdouh, A., Krishna Sarkar, A., Agrawal, A., Kumar, R. & Ahmad Khan, R. (2020, May 13). Healthcare Data Breaches: Insights and Implications. https://pmc.ncbi.nlm.nih.gov/articles/PMC7349636

Information Systems Audit and Control Association. (2010, January). Performing a Security Risk Assessment. https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment?gad_source=1&gclid=Cj0KCQjwxsm3BhDrARIsAMtVz6PQMZVCW1k5Nb8rnoLhJWDXxBMYUqrlnztZSGsICmZu2pkUXHEvv5gaApmtEALw_wcB

INSURICA Insurance Management Network. (2024). Cyber Case Study: Colonial Pipeline Ransomware Attack. https://insurica.com/blog/colonial-pipeline-ransomware-attack/

International Business Machines. (2025). Cost of a Data Breach Report 2025. https://www.ibm.com/reports/data-breach

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001

Janardhan, S. (2021, October 5). More details about the October 4 outage. https://engineering.fb.com/2021/10/05/networking-traffic/outage-details

Jijo George, K., Sivabalan1, A, Prabhu, T. & Anand Prasad, R. (2015 May 1). End-to-End Mobile Communication Security Testbed Using Open Source. Applications in Virtual Environmenthttps://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_314.pdf

Khaki Kaleba, H. & Tembo, S. (2025, November). Quantitative Cyber Risk Assessment for Critical Infrastructure in Zambia: A Bayesian Network Approach. https://www.researchgate.net/publication/398039428_Quantitative_Cyber_Risk_Assessment_for_Critical_Infrastructure_in_Zambia_A_Bayesian_Network_Approach

Kreso, I. (2025, October 16). Cyber Threats and Vulnerability Mapping in the Energy Sector: Laying the Groundwork for Smart Grid Resilience. https://www.acigjournal.com/pdf-211124-131512?filename=Cyber-Threats-and-Vulnera.pdf

Kumar Balaraman, N., Patel, K. & Reddy, N. (2025). Smart Water Management: Integrating PLC and SCADA Technologies for Sustainable Urban Infrastructure. https://www.scitepress.org/Papers/2025/137580/137580.pdf

Liveri, D., Sarri, A. & Skouloudi C. (2015). Security and Resilience in eHealth. https://www.enisa.europa.eu/sites/default/files/publications/Security%20and%20Resilience%20in%20eHealth%20Infrastructures%20and%20Services.pdf

Lo, J. & Bouarfa, J. (2021, January). Evaluating Airline and Railway Command and Control Systems. https://www.researchgate.net/publication/348243116_Evaluating_Airline_and_Railway_Command_and_Control_Systems

Mell, P. & Grance, T. (2011, September). The NIST Definition of Cloud Computing. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Moore, M. (n.d.). Top Cybersecurity Threats to Watch in 2026. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

Morgan, S. & Sausalito, C. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/cybercrime-damage-costs

Mulugeta Melaku, H. (2023, Jun 09). Context-Based and Adaptive Cybersecurity Risk Management Framework. https://encyclopedia.pub/entry/45315

Myung Song, J., Wang, T., Ju-Chun, Y. & Yu-Hung, C. (2024, July 11). Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains? https://www.sciencedirect.com/science/article/abs/pii/S1467089524000289

National Institute of Standards and Technology. (2024, February 26). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology. (2018, December). Risk Management Framework for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Institute of Standards and Technology. (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

National Institute of Standards and Technology. (2012, September). Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Nawaz Khan, W., Kyu Lee, J & Liu, S. (2025, January 15). Is Cybersecurity a Social Responsibility? https://link.springer.com/article/10.1007/s10796-024-10565-z

Nurthen, J. M. (2023, September). Cybersecurity Risk Assessment Matrix (CRAM): A System-Theoretic Approach to Balancing Operational and Cybersecurity Risk in the Management of Transient Cyber Assets (TCA) in the Maintenance of Operational Technology (OT). https://dspace.mit.edu/bitstream/handle/1721.1/152760/nurthen-johnmn40-sm-sdm-2023-thesis.pdf

Organisation for Economic Co-operation and Development. (2024, December 12). DIGITAL PUBLIC INFRASTRUCTURE FOR DIGITAL GOVERNMENTS. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf

Organisation for Economic Co-operation and Development. (2022). OECD Policy Framework on Digital Security. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

Othihiwa, A., Olayinka, O., Asuni, L. & Aluko, S. (2025, June). Modernising Core Banking Systems.

https://assets.kpmg.com/content/dam/kpmg/ng/pdf/2025/06/Modernising%20Core%20Banking%20Systems.pdf

Paganini, P. (2017, November 14). DHS – Tests demonstrate Boeing 757 airplanes vulnerable to hacking. https://www.cyberdefensemagazine.com/dhs-tests-demonstrate-boeing-757-airplanes-vulnerable-to-hacking/

Patchamatla, P. S. (2014). Quantitative Vendor Risk Scoring in Telecommunications Using Integrated Governance Frameworks. https://saspublishers.com/media/articles/SJET_26B_857-865.pdf

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J. & PeerenboomÖ J. (2015, June). Analysis of Critical Infrastructure Dependencies and Interdependencies. https://publications.anl.gov/anlpubs/2015/06/111906.pdf

Pinzariu, N. & Anagnostakis, D. (2022). Cyber Security Risk Assessment for Advanced Manufacturing. https://hvm.catapult.org.uk/wp-content/uploads/2022/07/HVMC_Cyber-Security-Report_Full.pdf

Ramage, X., Lebea, K. & Sithungu, S. (2025, June). Cyber Warfare and Critical Infrastructure. https://www.researchgate.net/publication/393049584_Cyber_Warfare_and_Critical_Infrastructure

Reddy Palleti, V., Adepu, S., Kumar Mishra, V. & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. https://scispace.com/pdf/cascading-effects-of-cyber-attacks-on-interconnected-durlhc83vw.pdf

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. & McQuaid, R. (2021, December). Developing Cyber-Resilient Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

Sadiku, M. N. O., Adekunte, P. A. & Sadiku, J. O. (2024, December). Cybersecurity in Telecommunications. https://www.ijtsrd.com/papers/ijtsrd71623.pdf

Saleem, M. Parmar, H. & Kassar, G. R. (2026, January 24). Protection Of Critical Infrastructure against Cyber Attacks: An International Law Perspective. https://ssrn.com/abstract=6072848

Saropa Contacts News. (2025, December 4). No Cash, No Service, No 911: The Day Rogers Failed. Saropa. https://saropa-contacts.medium.com/no-cash-no-service-no-911-the-day-rogers-failed-3cfbb06a6a53

Saudi Arabian Monetary Authority. (2017, May). Cyber Security Framework. https://rulebook.sama.gov.sa/sites/default/files/en_net_file_store/SAMA_EN_3837_VER1.pdf

Shankar, N. (2024, February 21). The Biden Administration's National Cybersecurity Strategy: Opportunities and Challenges. https://mei.edu/publication/biden-administrations-national-cybersecurity-strategy-opportunities-and-challenges/

Sheehan, B., Murphy, F., Kia, A. N. & Kiely, R. (2021, Mar 23). A quantitative bow-tie cyber risk classification and assessment framework. https://www.tandfonline.com/doi/full/10.1080/13669877.2021.1900337#abstract

Shukla, M., Johnson, S. & Jones, P. (2025, April 30). Cascading impacts to critical national infrastructure in connected places triggered by cyber-attacks on smart EV charging infrastructure. https://academic.oup.com/iti/article/doi/10.1093/iti/liaf007/8122270?

SKYbrary Aviation Safety. (n.d.). GNSS Jamming and Spoofing. https://skybrary.aero/articles/gnss-jamming-and-spoofing

Tatar, U., Keskin, O., Bahsi, H. & Ariel Pinto, C. (2020, May). Quantification of Cyber Risk for Actuaries. https://www.casact.org/sites/default/files/2021-02/soa_cyber_risk_v3_final.pdf

The White House. (2013, February 12). Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Toregas, C. & Santos, M. (2019). Cybersecurity and its cascading effect on societal systems. https://www.undrr.org/publication/cybersecurity-and-its-cascading-effect-societal-systems

Tripathi, A. (2025, August). Evaluating the Role of Confidentiality, Integrity, and Availability in Cyber Defence. https://www.ijirmps.org/papers/2025/4/232662.pdf

United Nations Children's Fund. (n.d.). Stepwise toolkit on cybersecurity, confidentiality, and privacy for planning and operationalizing patientcentric digital health systems. https://www.unicef.org/digitalimpact/media/706/file/Stepwise%20toolkit%20on%20cybersecurity%20confidentiality%20and%20privacy.pdf

U.S. Government Accountability Office. (2025, February). Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness. https://files.gao.gov/reports/GAO-25-107743/index.html

U. S. Government Accountability Office. (2009, July 17). Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD's Tier 1 Task Critical Asset List. https://www.gao.gov/assets/a96309.html

U. S. Office of the Under Secretary of Defense for Policy. (2016, November 29). DOD DIRECTIVE 3020.40 MISSION ASSURANCE (MA). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf

Xona Partners Inc. (2023, December 12). Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage. https://publications.gc.ca/collections/collection_2024/crtc/BC92-130-1-2024-eng.pdf

Yoo, Y. & Han-Seon, P. (2021, May 24). Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. https://www.mdpi.com/2077-1312/9/6/565

Zadeh, A., Lavine, B., Zolbanin, H. & Hopkins, D. (2023, December). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. https://www.sciencedirect.com/science/article/pii/S2772662223001686

Zahidi, S., Cavaciuti-Wishart, E., Heading, S. & Kohler, K. (2024, January). Global Risks Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Zurich Insurance Group. (2025, October 2). and Cyber Threat Alliance. Cyber metrics for key decision-makers. Retrieved April 05, 2026, from https://www.cyberthreatalliance.org/wp-content/uploads/2025/10/2509GC-CyberMetrics-Brochure-final-v1-1.pdf

Table 1

Risk Matrix

Likelihood\ Impact	1	2	3	4	5
5	Medium	High	High	Critical	Critical
4	Medium	Medium	High	High	Critical
3	Low	Medium	Medium	High	High
2	Low	Low	Medium	Medium	High
1	Very Low	Low	Low	Medium	Medium

Table 2

Security Domain Control Score

Security Domain	Control Score
Governance & policy	4 (Managed and monitored)
Asset management	2 (Basic controls exist)
Network security	4 (Managed and monitored)
Identity & access management	3 (Documented processes)
Threat detection & monitoring	5 (Continuous improvement)
Incident response	4 (Managed and monitored)
Vulnerability management	3 (Documented processes)
Backup & resilience	4 (Continuous improvement)

Table 3

Control Score

Control	Score
No formal controls	1
Basic controls exist	2
Documented processes	3
Managed and monitored	4
Continuous improvement	5

Table 4

Maturity Level

Maturity Level	Security Maturity Reduction Value
Level 1	Initial = 0
Level 2	Developing = 5
Level 3	Defined = 10
Level 4	Managed = 15
Level 5	Advanced = 20
Level 6	Optimized = 25

Table 5

Risk Level

Risk Level	Level
0–5	Very Low
6–15	Low
16–25	Medium
26–40	High
41–50	Critical