UpGuard™

DORA Assessment Workbook

Use this workbook to map relevant controls from the NIST CSF and ISO 27001 frameworks to the five main pillars of the DORA.

Trusted by hundreds of companies worldwide

PagerDuty NYSE hopin iag ICE TDK

UpGuard

ICT Risk Management

ICT Risk Management	NIST CSF	
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	Implemented: Yes Partially No Implementation Details Mitigation Actions
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	Implemented: Yes Partially No Implementation Details Mitigation Actions
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	Implemented: Yes Partially No Implementation Details Mitigation Actions

UpGuard

ICT Risk Management

GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

UpGuard

ICT Risk Management

GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

ICT Risk Management

GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

ICT Risk Management

GV.OV-01:

Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

GV.OV-02:

The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

GV.OV-03:

Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ID.RA-05:

Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ICT Risk Management

ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

ICT Risk Management	ISO 27001	
	Clause 6.1: Actions to address risks and opportunities (including all sub-clauses)	Implemented: ◯ Yes ◯ Partially ◯ No Implementation Details Mitigation Actions
	Clause 8: Operation (including all sub-clauses)	Implemented: ◯ Yes ◯ Partially ◯ No Implementation Details Mitigation Actions

UpGuard

ICT-Related Incident Response

ICT-Related Incident Response

NIST CSF	
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	Implemented: Yes Partially No Implementation Details Mitigation Actions
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Implemented: Yes Partially No Implementation Details Mitigation Actions
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Implemented: Yes Partially No Implementation Details Mitigation Actions

ICT-Related Incident Response

GV.SC-08:	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Implemented: Yes Partially No Implementation Details Mitigation Actions
ID.IM-04:	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Implemented: Yes Partially No Implementation Details Mitigation Actions
DE.AE-08:	Incidents are declared when adverse events meet the defined incident criteria	Implemented: Yes Partially No Implementation Details Mitigation Actions
RS.MA-01:	The incident response plan is executed in coordination with relevant third parties once an incident is declared	Implemented: Yes Partially No Implementation Details Mitigation Actions

ICT-Related Incident Response

RS.MA-02:

Incident reports are triaged and validated.

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RS.MA-03:

Incidents are categorized and prioritized

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RS.MA-04:

Incidents are escalated or elevated as needed

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RS.MA-05:

The criteria for initiating incident recovery are applied

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ICT-Related Incident Response

RS.AN-03:

Analysis is performed to establish what has taken place during an incident and the root cause of the incident

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RS.AN-06:

Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RS.AN-07:

Incident data and metadata are collected, and their integrity and provenance are preserved

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RS.AN-08:

An incident's magnitude is estimated and validated

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ICT-Related Incident Response	RS.CO-02: Internal and external stakeholders are notified of incidents	Implemented: Yes Partially No Implementation Details Mitigation Actions
	RS.CO-03: Information is shared with designated internal and external stakeholders	Implemented: Yes Partially No Implementation Details Mitigation Actions
	RS.MI-01: Incidents are contained	Implemented: Yes Partially No Implementation Details Mitigation Actions
	RS.MI-02: Incidents are eradicated	Implemented: Yes Partially No Implementation Details Mitigation Actions

ICT-Related Incident Response

RC.RP-01:

The recovery portion of the incident response plan is executed once initiated from the incident response process

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RC.RP-02:

Recovery actions are selected, scoped, prioritized, and performed

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RC.RP-03:

The integrity of backups and other restoration assets is verified before using them for restoration

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RC.RP-04:

Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ICT-Related Incident Response

RC.RP-05:

The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RC.RP-06:

The end of incident recovery is declared based on criteria, and incidentrelated documentation is completed

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RC.CO-03:

Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

RC.CO-04:

Public updates on incident recovery are shared using approved methods and messaging

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ICT-Related Incident Response	ISO 27001	
	A.5.24: Information security incident management planning and preparation	Implemented: Yes Partially No Implementation Details Mitigation Actions
	A.5.25: Assessment and decision on information security events	Implemented: Yes Partially No Implementation Details Mitigation Actions
	A.5.26: Response to information security incidents	Implemented: Yes Partially No Implementation Details Mitigation Actions
	A.5.27: Learning from information security incidents	Implemented: Yes Partially No Implementation Details Mitigation Actions

	A.5.28: Collection of evidence	Implemented: ◯ Yes ◯ Partially ◯ No Implementation Details Mitigation Actions

UpGuard

Digital Operational Resilience Testing

Digital Operational Resilience Testing

NIST CSF	
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

Digital Operational Resilience Testing

ID.RA-03:

Internal and external threats to the organization are identified and recorded

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ID.IM-04:

Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

PR.IR-02:

The organization's technology assets are protected from environmental threats

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

PR.IR-03:

Mechanisms are implemented to achieve resilience requirements in normal and adverse situations

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

Digital Operational Resilience Testing	**PR.IR-04:** Adequate resource capacity to ensure availability is maintained	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

Digital Operational Resilience Testing	ISO 27001	
	A.5.29: Information security during disruption	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	A.5.30: ICT readiness for business continuity	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

UpGuard

ICT Third-Party Risk

ICT Third-Party Risk

NIST CSF	
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Implemented: Yes Partially No Implementation Details Mitigation Actions
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Implemented: Yes Partially No Implementation Details Mitigation Actions
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Implemented: Yes Partially No Implementation Details Mitigation Actions

ICT Third-Party Risk

GV.SC-04:

Suppliers are known and prioritized by criticality

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

GV.SC-05:

Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

GV.SC-06:

Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

GV.SC-07:

The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ICT Third-Party Risk

GV.SC-09:

Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

GV.SC-10:

Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ID.AM-03:

Representations of the organization's authorized network communication and internal and external network data flows are maintained

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ID.AM-04:

Inventories of services provided by suppliers are maintained

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

ICT Third-Party Risk

ID.AM-05:

Assets are prioritized based on classification, criticality, resources, and impact on the mission

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ID.RA-09:

The authenticity and integrity of hardware and software are assessed prior to acquisition and use

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ID.RA-10:

Critical suppliers are assessed prior to acquisition

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

PR.AA-01:

Identities and credentials for authorized users, services, and hardware are managed by the organization

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ICT Third-Party Risk

PR.AA-02:

Identities are proofed and bound to credentials based on the context of interactions

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

PR.AA-03:

Users, services, and hardware are authenticated

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

PR.AA-05:

Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

PR.AA-06:

Physical access to assets is managed, monitored, and enforced commensurate with risk

Implemented: ○ Yes ○ Partially ○ No

Implementation Details

Mitigation Actions

ICT Third-Party Risk

ISO 27001	
A.5.19: Information security in supplier agreements	Implemented: Yes Partially No Implementation Details Mitigation Actions
A.5.20: Addressing information security within supplier agreements	Implemented: Yes Partially No Implementation Details Mitigation Actions
A.5.21: Managing information security in the information and communication technology (ICT) supply chain	Implemented: Yes Partially No Implementation Details Mitigation Actions
A.5.22: Monitoring, review, and change management of supplier services	Implemented: Yes Partially No Implementation Details Mitigation Actions

A.5.23:

Information security for use of cloud services

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

UpGuard

Information Sharing

Information Sharing	NIST CSF	
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Implemented: Yes Partially No Implementation Details Mitigation Actions
	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	Implemented: Yes Partially No Implementation Details Mitigation Actions
	ID.RA-03: Internal and external threats to the organization are identified and recorded	Implemented: Yes Partially No Implementation Details Mitigation Actions

Information Sharing	**RS.CO-02:** Internal and external stakeholders are notified of incidents	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	RS.CO-03: Information is shared with designated internal and external stakeholders	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions
	RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	Implemented: ○ Yes ○ Partially ○ No Implementation Details Mitigation Actions

	ISO 27001	
Information Sharing	A.5.5: Contact with authorities	Implemented: Yes Partially No Implementation Details Mitigation Actions
	A.5.6: Contact with special interest groups	Implemented: Yes Partially No Implementation Details Mitigation Actions
	A.5.7: Threat intelligence	Implemented: Yes Partially No Implementation Details Mitigation Actions
	A.5.14: Information transfer	Implemented: Yes Partially No Implementation Details Mitigation Actions

A.5.31:

Legal, statutory, regulatory and contractual requirements

Implemented: Yes Partially No

Implementation Details

Mitigation Actions

UpGuard

How UpGuard helps organizations comply with the DORA framework

UpGuard provides automatic compliance mapping and reporting against DORA through NIST CSF and ISO 27001 for you and your vendors. Assess your DORA compliance today.

Free Trial →

Trusted by hundreds of companies worldwide

PagerDuty NYSE hopin iag ICE TDK

www.upguard.com

+1 888-882-3223

650 Castro Street, Suite 120-387, Mountain View CA 94041 United States