# Roger Insurance ISO 27001 2022 Readiness Report

August 19, 2024

Please note, this report was prepared by Cynomi platform for the purpose of initial evaluation. Cynomi does not take responsibility for or relating to the information included in this document or its accuracy and offers no warranty.

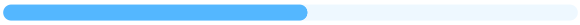
Powered by cynomi

# ISO 27001 2022 Compliance Report

🟦 Company coverage

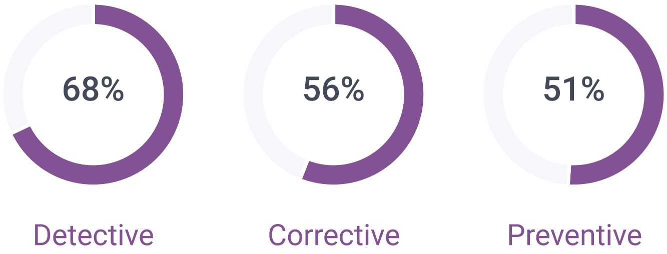
▭ Total controls

**ISO 27001 2022**

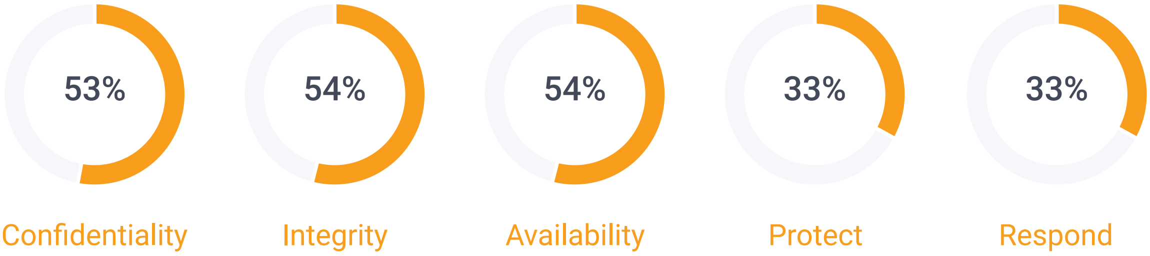


53% completed

## Control type

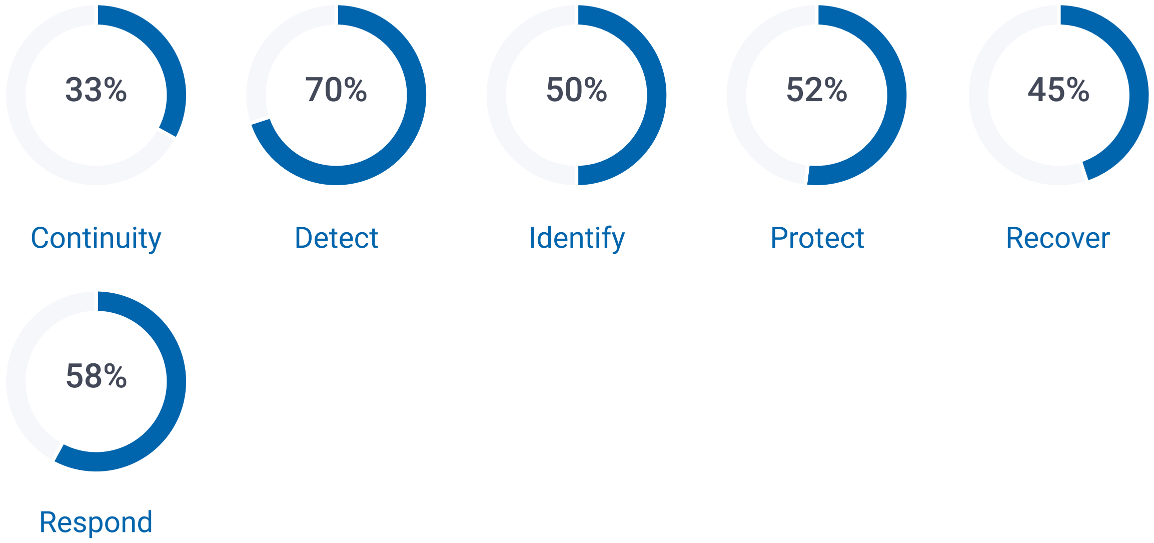


## Information security properties

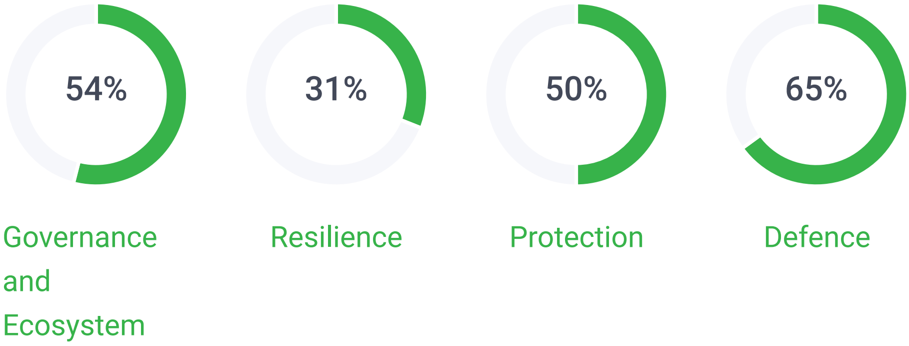


# ISO 27001 2022 Compliance Report

## Cybersecurity concepts



## Security domain



# ISO 27001 2022 Compliance Report

## Detailed Report

This report details your organization's compliance status with the framework, for the purpose of initial evaluation. This status is based on information provided by you about your organization.

| CONTROL | NAME | CONTROL STATUS |
|---|---|---|
| A.5.1 | Policies for information security | Not Implemented |
| A.5.10 | Acceptable use of information and other associated assets | Implemented |
| A.5.11 | Return of assets | Implemented |
| A.5.12 | Classification of information | Partially |
| A.5.13 | Labelling of information | Implemented |
| A.5.14 | Information transfer | Not Implemented |
| A.5.15 | Access control | Partially |
| A.5.16 | Identity management | Partially |
| A.5.17 | Authentication information | Partially |
| A.5.18 | Access rights | Partially |
| A.5.19 | Information security in supplier relationships | Not Implemented |
| A.5.2 | Information security roles and responsibilities | Implemented |
| A.5.20 | Addressing information security within supplier agreements | Not Implemented |
| A.5.21 | Managing information security in the ICT supply chain | Not Implemented |
| A.5.22 | Monitoring, review and change management of supplier services | Implemented |
| A.5.23 | Information security for use of cloud services | Partially |

# ISO 27001 2022 Compliance Report

| CONTROL | NAME | CONTROL STATUS |
|---|---|---|
| A.5.24 | Information security incident management planning and preparation | Partially |
| A.5.25 | Assessment and decision on information security events | Implemented |
| A.5.26 | Response to information security incidents | Implemented |
| A.5.27 | Learning from information security incidents | N/A |
| A.5.28 | Collection of evidence | Implemented |
| A.5.29 | Information security during disruption | Partially |
| A.5.3 | Segregation of duties | Implemented |
| A.5.30 | ICT readiness for business continuity | Partially |
| A.5.31 | Legal, statutory, regulatory and contractual requirements | Partially |
| A.5.32 | Intellectual property rights | Implemented |
| A.5.33 | Protection of records | Partially |
| A.5.34 | Privacy and protection of PII | Implemented |
| A.5.35 | Independent review of information security | Implemented |
| A.5.36 | Compliance with policies, rules and standards for information security | Partially |
| A.5.37 | Documented operating procedures | Implemented |
| A.5.4 | Management responsibilities | Implemented |
| A.5.5 | Contact with authorities | Not Implemented |
| A.5.6 | Contact with special interest groups | Not Implemented |

# ISO 27001 2022 Compliance Report

| CONTROL | NAME | CONTROL STATUS |
|---|---|---|
| A.5.7 | Threat intelligence | Partially |
| A.5.8 | Information security in project management | Not Implemented |
| A.5.9 | Inventory of information and other associated assets | Partially |
| A.6.1 | Screening | Implemented |
| A.6.2 | Terms and conditions of employment | Partially |
| A.6.3 | Information security awareness, education and training | Implemented |
| A.6.4 | Disciplinary process | Partially |
| A.6.5 | Responsibilities after termination or change of employment | Not Implemented |
| A.6.6 | Confidentiality or non-disclosure agreements | Not Implemented |
| A.6.7 | Remote working | Implemented |
| A.6.8 | Information security event reporting | Partially |
| A.7.1 | Physical security perimeters | Not Implemented |
| A.7.10 | Storage media | Not Implemented |
| A.7.11 | Supporting utilities | Implemented |
| A.7.12 | Cabling security | Implemented |
| A.7.13 | Equipment maintenance | Not Implemented |
| A.7.14 | Secure disposal or re-use of equipment | Not Implemented |
| A.7.2 | Physical entry | Partially |

# ISO 27001 2022 Compliance Report

| CONTROL | NAME | CONTROL STATUS |
|---|---|---|
| A.7.3 | Securing offices, rooms and facilities | Not Implemented |
| A.7.4 | Physical security monitoring | Partially |
| A.7.5 | Protecting against physical and environmental threats | Partially |
| A.7.6 | Working in secure areas | Not Implemented |
| A.7.7 | Clear desk and clear screen | Not Implemented |
| A.7.8 | Equipment siting and protection | Not Implemented |
| A.7.9 | Security of assets off-premises | Not Implemented |
| A.8.1 | User endpoint devices | Partially |
| A.8.10 | Information deletion | Implemented |
| A.8.11 | Data masking | Implemented |
| A.8.12 | Data leakage prevention | Partially |
| A.8.13 | Information backup | Partially |
| A.8.14 | Redundancy of information processing facilities | Not Implemented |
| A.8.15 | Logging | Partially |
| A.8.16 | Monitoring activities | Partially |
| A.8.17 | Clock synchronization | Implemented |
| A.8.18 | Use of privileged utility programs | Not Implemented |
| A.8.19 | Installation of software on operational systems | Implemented |

# ISO 27001 2022 Compliance Report

| CONTROL | NAME | CONTROL STATUS |
|---|---|---|
| A.8.2 | Privileged access rights | Implemented |
| A.8.20 | Networks security | Partially |
| A.8.21 | Security of network services | Implemented |
| A.8.22 | Segregation of networks | Implemented |
| A.8.23 | Web filtering | Implemented |
| A.8.24 | Use of cryptography | Implemented |
| A.8.25 | Secure development life cycle | Not Implemented |
| A.8.26 | Application security requirements | Partially |
| A.8.27 | Secure system architecture and engineering principles | Not Implemented |
| A.8.28 | Secure coding | Partially |
| A.8.29 | Security testing in development and acceptance | Partially |
| A.8.3 | Information access restriction | Implemented |
| A.8.30 | Outsourced development | Partially |
| A.8.31 | Separation of development, test and production environments | Partially |
| A.8.32 | Change management | Not Implemented |
| A.8.33 | Test information | Not Implemented |
| A.8.34 | Protection of information systems during audit testing | Partially |
| A.8.4 | Access to source code | Implemented |

# ISO 27001 2022 Compliance Report

| CONTROL | NAME | CONTROL STATUS |
|---|---|---|
| A.8.5 | Secure authentication | Partially |
| A.8.6 | Capacity management | Partially |
| A.8.7 | Protection against malware | Partially |
| A.8.8 | Management of technical vulnerabilities | Partially |
| A.8.9 | Configuration management | Partially |