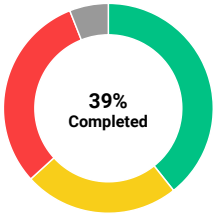
Vendor Asessment Results Printable Report

Rover Wire Steel Ltd

117 Controls



46	Covered
28	Partially Covered
36	Not Covered
7	Unsure
0	Not Assessed

CC1.4	CC1.5	CC4.7	CC4.8	CC4.9	CC5.1	CC5.5
CC6.1	CC6.2	CC7.2	CC7.3	CC7.4	CC7.7	CC7.8
CC7.9	CC7.10	CC7.11	CC7.12	CC7.13	CC7.14	CC7.15
CC7.16	CC7.17	CC7.18	CC7.19	CC7.20	CC7.21	CC7.22
CC7.23	CC7.24	CC7.25	CC7.27	CC7.29	CC7.30	CC7.31
CC7.32	CC7.33	CC7.34	CC7.35	CC7.36	CC7.37	CC7.38
CC7.39	CC8.16	CC8.18	CC8.19	CC8.20	CC8.24	CC8.26
CC8.30	CC8.32	CC8.33	CC8.34	CC8.35	CC8.36	CC8.37
CC8.38	CC8.39	CC8.40	CC8.41	CC8.42	CC8.43	CC8.44
CC8.45	CC8.46	CC8.47	CC8.48	CC9.2	CC9.3	CC9.7
CC9.8	CC9.9	CC9.10	CC10.1	CC10.3	CC10.4	CC10.5
CC10.6	CC10.7	CC10.8	CC10.9	CC11.2	CC11.5	CC11.6
CC11.7	CC11.8	CC11.9	CC11.10	CC11.11	CC11,12	CC11.15
CC12.1	CC12.2	CC12.3	CC12.4	CC12.5	CC12.6	CC13.3
CC13.5	CC13.6	CC13.8	CC13.9	CC13.10	CC13.11	CC13.12

CC13.13	CC14.19	CC15.1	CC16.1	CC16.2	CC16.5	CC17.1
CC17.3	CC18.12	CC18.15	CC19.2	CC19.16		

Data Flow Management

Ensure that a baseline of network operations and expected data flows for users and systems is established and managed.

Yes, Fully

Control Reference:

CC1.4

Comments:

No comments

Baseline Configurations

Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements) throughout the respective system development life cycles.

Yes, Fully

Control Reference:

CC1.5

Comments:

No comments

System Security Plans (SSP)/Written Information Security Plans (WISP)/Information Security Management System (ISMS)

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Yes, Partially

Control Reference:

CC4.7

Comments:

No comments

Security Control Effectiveness

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Yes, Partially

Control Reference:

CC4.8

Comments:

No comments

Security Plans of Action

Develop and implement plans of action with timelines designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Yes, Fully

Control Reference:

CC4.9

Comments:

No comments

Risk Assessment/Risk Analysis

Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.

No

Control Reference:

CC5.1

Comments:

No comments

Monitor Security Controls

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Yes, Fully

Control Reference:

CC5.5

Comments:

No comments

Screen Individuals

Screen individuals prior to authorizing access to organizational systems.

Unsure

Control Reference:

CC6.1

Comments:

No comments

Terminations & Transfers

Yes, Fully

Ensure that organizational systems are protected during and after personnel actions such as terminations and transfers.

Control Reference:

CC6.2

Comments:

No comments

Physical Access Management

Yes, Partially

Manage and protect physical access to assets.

Control Reference:

CC7.2

Comments:

No comments

Remote Access Management

No

Manage remote access to assets.

Control Reference:

CC7.3

Comments:

No comments

Access Permission Management

Yes, Fully

Manage access permissions, incorporating the principles of least privilege and separation of duties.

Control Reference:

CC7.4

Comments:

No comments

Unique User Identification

Yes, Partially

Assign a unique name and/or number for identifying and tracking user identity.

Control Reference:

CC7.7

Comments:

No comments

Identity Authentication

No

Implement procedures to verify that a person or entity seeking access to data is the one claimed.

Control Reference:

CC7.8

Comments:

No comments

Workforce Authorization & Supervision

Unsure

Implement procedures for the authorization and/or supervision of workforce members.

Control Reference:

CC7.9

Comments:

No comments

Appropriate Access

No

Implement procedures to determine that the access of a workforce member is appropriate.

Control Reference:

CC7.10

Comments:

No comments

Access Termination

Yes, Partially

Implement procedures for terminating access when the employment of a workforce member ends or as required by other determinations.

Control Reference:

CC7.11

Comments:

No comments

Limit Access

Yes, Fully

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Control Reference:

CC7.12

Comments:

No comments

Limit Functions

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Yes, Fully

Control Reference:

CC7.13

Comments:

No comments

Control External Information Systems

Verify and control/limit connections to and use of external information systems.

Yes, Partially

Control Reference:

CC7.14

Comments:

No comments

Control Publicly Accessible Systems

Control information posted or processed on publicly accessible information systems.

No

Control Reference:

CC7.15

Comments:

No comments

Identify System Users

Identify information system users, processes acting on behalf of users, or devices.

Unsure

Control Reference:

CC7.16

Comments:

No comments

Escort & Monitor Visitors

Escort visitors and monitor visitor activity.

Yes, Partially

Control Reference:

CC7.17

Comments:

No comments

Facility Security Plan

Implement documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Yes, Fully

Control Reference:

CC7.18

Comments:

No comments

Physical Access Devices

Control and manage physical access devices.

Yes, Fully

Control Reference:

CC7.19

Comments:

No comments

Physical Access Logs

Maintain audit logs of physical access.

Yes, Fully

Control Reference:

CC7.20

Comments:

No comments

Privacy & Security Notices

Provide privacy and security notices consistent with applicable rules.

Yes, Partially

Control Reference:

CC7.21

Comments:

No comments

Limit Portable Storage Devices

Limit use of portable storage devices on external systems.

Yes, Fully

Control Reference:

CC7.22

Comments:

No comments

Using Privileged Accounts

Use non-privileged accounts or roles when accessing nonsecurity functions. Use privileged accounts only when performing functions requiring them.

No

Control Reference:

CC7.23

Comments:

No comments

Limit Unsuccessful Logons

Limit unsuccessful logon attempts.

Yes, Fully

Control Reference:

CC7.24

Comments:

No comments

Authorize Wireless Access

Authorize wireless access prior to allowing such connections.

Yes, Partially

Control Reference:

CC7.25

Comments:

No comments

Manage Remote Access

Route remote access via managed access control points.

No

Control Reference:

CC7.27

Comments:

No comments

Privileged Functions

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Yes, Partially

Control Reference:

CC7.29

Comments:

No comments

Terminate Sessions

Terminate (automatically) user sessions after a defined condition.

Yes, Fully

Control Reference:

CC7.30

Comments:

No comments

Wireless Authentication & Encryption

Protect wireless access using authentication and encryption.

Yes, Fully

Control Reference:

CC7.31

Comments:

No comments

Mobile Device Control

Control connection of mobile devices.

No

Control Reference:

CC7.32

Comments:

No comments

Encrypt Remote Sessions

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Yes, Partially

Control Reference:

CC7.33

Comments:

No comments

Authorize Privileged Remote Sessions

Authorize remote execution of privileged commands and remote access to security-relevant information.

Yes, Fully

Control Reference:

CC7.34

Comments:

No comments

Encrypt Mobile Devices

Encrypt data on mobile devices and mobile computing platforms.

Yes, Fully

Control Reference:

CC7.35

Comments:

No comments

Multifactor Authentication (MFA)

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Yes, Partially

Control Reference:

CC7.36

Comments:

No comments

Replay-resistant Authentication

Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.

Yes, Fully

Control Reference:

CC7.37

Comments:

No comments

Prevent Identifier Reuse

Prevent the reuse of identifiers for a defined period.

Yes, Fully

Control Reference:

CC7.38

Comments:

No comments

Disable Identifiers

Disable identifiers after a defined period of inactivity.

Yes, Fully

Control Reference:

CC7.39

Comments:

No comments

Control & Limit Access

Yes, Fully

Ensure that access to systems and assets is controlled, incorporating the principle of least functionality.

Control Reference:

CC8.16

Comments:

No comments

Install Patches & Updates

Yes, Partially

Ensure that all software and firmware are updated with patches and updates within 7 days of becoming available, unless warnings indicate a faster implementation is required.

Control Reference:

CC8.18

Comments:

No comments

Firewall Protection

No

Ensure that firewalls with active intrusion prevention protect the perimeter of the network.

Control Reference:

CC8.19

Comments:

No comments

Malicious Software Protection & Detection

Yes, Partially

Implement procedures for guarding against, detecting, and reporting malicious software.

Control Reference:

CC8.20

Comments:

No comments

Disposal

Yes, Partially

Implement policies and procedures to address the final disposition of electronic data and/or the hardware or electronic media on which it is stored.

Control Reference:

CC8.24

Comments:

No comments

Terminate Sessions

Yes, Fully

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Control Reference:

CC8.26

Comments:

No comments

Update Protection

Yes, Partially

Update malicious code protection mechanisms when new releases are available.

Control Reference:

CC8.30

Comments:

No comments

User-installed Software

Yes, Partially

Control and monitor user-installed software.

Control Reference:

CC8.32

Comments:

No comments

Security Configurations

Yes, Fully

Establish and enforce security configuration settings for information technology products employed in organizational systems.

Control Reference:

CC8.33

Comments:

No comments

Manage Changes

Yes, Fully

Track, review, approve, or disapprove, and log changes to organizational systems.

Control Reference:

CC8.34

Comments:

No comments

Impact Planning

Yes, Fully

Analyze the security impact of changes prior to implementation.

Control Reference:

CC8.35

Comments:

No comments

Minimum Password Complexity

No

Enforce a minimum password complexity and change of characters when new passwords are created.

Control Reference:

CC8.36

Comments:

No comments

Prohibit Password Reuse

Yes, Partially

Prohibit password reuse for a specified number of generations.

Control Reference:

CC8.37

Comments:

No comments

Temporary Passwords

Yes, Fully

Allow temporary password use for system logons with an immediate change to a permanent password.

Control Reference:

CC8.38

Comments:

No comments

Encrypt Passwords

Yes, Partially

Store and transmit only cryptographically-protected passwords.

Control Reference:

CC8.39

Comments:

No comments

Obscure Authentication Information

Obscure feedback of authentication information.

Yes, Fully

Control Reference:

CC8.40

Comments:

No comments

Incident Management Process

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

No

Control Reference:

CC8.41

Comments:

No comments

Scan Files

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Yes, Fully

Control Reference:

CC8.42

Comments:

No comments

Monitor Security Alerts

Monitor system security alerts and advisories and take action in response.

Yes, Fully

Control Reference:

CC8.43

Comments:

No comments

Monitor Systems

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Yes, Fully

Control Reference:

CC8.44

Comments:

No comments

Change Security

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Yes, Fully

Control Reference:

CC8.45

Comments:

No comments

Restrict Nonessential Resources

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Yes, Fully

Control Reference:

CC8.46

Comments:

No comments

Blacklisting

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Yes, Fully

Control Reference:

CC8.47

Comments:

No comments

Protect Controlled Unclassified Information (CUI)

Protect the confidentiality of CUI at rest.

No

Control Reference:

CC8.48

Comments:

No comments

Perform & Control Maintenance & Repairs

Ensure maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.

No

Control Reference:

CC9.2

Comments:

No comments

Control Maintenance

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

No

Control Reference:

CC9.3

Comments:

No comments

Remote Maintenance Sessions

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

No

Control Reference:

CC9.7

Comments:

No comments

Supervise Maintenance Activities

Supervise the maintenance activities of personnel without required access authorization.

Yes, Fully

Control Reference:

CC9.8

Comments:

No comments

Control Off-site Maintenance

Ensure equipment removed for off-site maintenance is sanitized of any sensitive or protected data.

Yes, Partially

Control Reference:

CC9.9

Comments:

No comments

Check Diagnostic Programs

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Yes, Fully

Control Reference:

CC9.10

Comments:

No comments

Implement Logging/Audit Controls

Ensure that audit/log records are implemented to record and examine activities on local devices, network devices, and cloud services.

Yes, Fully

Control Reference:

CC10.1

Comments:

No comments

Review Log Records

Ensure that audit/log records are reviewed regularly to identify unusual or unauthorized activity.

Yes, Fully

Control Reference:

CC10.3

Comments:

No comments

Synchronize System Clocks

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Yes, Fully

Control Reference:

CC10.4

Comments:

No comments

Logging Failure Alerts

Alert in the event of an audit logging process failure.

Yes, Fully

Control Reference:

CC10.5

Comments:

No comments

Protect Audit Information

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Yes, Partially

Control Reference:

CC10.6

Comments:

No comments

Limit Log Management

Yes, Partially

Limit management of audit logging functionality to a subset of privileged users.

Control Reference:

CC10.7

Comments:

No comments

Correlate Log Records

Yes, Fully

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Control Reference:

CC10.8

Comments:

No comments

Log Reduction & Report Generation

No

Provide audit record reduction and report generation to support on-demand analysis and reporting.

Control Reference:

CC10.9

Comments:

No comments

Control Physical Access

No

Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control.

Control Reference:

CC11.2

Comments:

No comments

Restrict Physical Access

Yes, Partially

Implement physical safeguards for all workstations and operating environments to restrict access to authorized users.

Control Reference:

CC11.5

Comments:

No comments

Facility Protection & Monitoring

No

Protect and monitor the physical facility and support infrastructure for organizational systems.

Control Reference:

CC11.6

Comments:

No comments

FIPS Encryption

No

Employ FIPS-validated cryptography when used to protect the confidentiality of data.

Control Reference:

CC11.7

Comments:

No comments

Employ Protection Principles

Yes, Partially

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Control Reference:

CC11.8

Comments:

No comments

Limit User Functionality

Yes, Fully

Separate user functionality from system management functionality.

Control Reference:

CC11.9

Comments:

No comments

Prevent Unauthorized/Unintended Data Transfer

Unsure

Prevent unauthorized and unintended information transfer via shared system resources.

Control Reference:

CC11.10

Comments:

No comments

Manage Encryption Keys

Establish and manage cryptographic keys for cryptography employed in organizational systems.

Unsure

Control Reference:

CC11.11

Comments:

No comments

Control & Monitor Mobile Code

Control and monitor the use of mobile code.

Unsure

Control Reference:

CC11,12

Comments:

No comments

Safeguard Alternate Work Sites

Enforce safeguarding measures for data at alternate work sites.

No

Control Reference:

CC11.15

Comments:

No comments

Sanitize Media

Sanitize or destroy information system media containing data before disposal or release for reuse.

Yes, Partially

Control Reference:

CC12.1

Comments:

No comments

Protect Physical Media

Protect (i.e., physically control and securely store) system media, both paper and digital.

No

Control Reference:

CC12.2

Comments:

No comments

Control Removable Media

Unsure

Control the use of removable media on system components. Prohibit the use of portable storage devices when such devices have no identifiable owner.

Control Reference:

CC12.3

Comments:

No comments

Mark Media

No

Mark media with necessary markings and distribution limitations.

Control Reference:

CC12.4

Comments:

No comments

Control Media Transport

No

Control access to media containing data and maintain accountability for media during transport outside of controlled areas.

Control Reference:

CC12.5

Comments:

No comments

Encrypt Media During Transport

Yes, Partially

Implement cryptographic mechanisms to protect the confidentiality of data stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Control Reference:

CC12.6

Comments:

No comments

Encryption of Data in Transit

No

Implement cryptographic mechanisms to prevent unauthorized disclosure of data during transmission unless otherwise protected by alternative physical safeguards.

Control Reference:

CC13.3

Comments:

No comments

Monitor, Control, and Protect Communications

Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

No

Control Reference:

CC13.5

Comments:

No comments

Implement Subnetworks

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

No

Control Reference:

CC13.6

Comments:

No comments

Control and Monitor Voice Communications

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Yes, Fully

Control Reference:

CC13.8

Comments:

No comments

Authenticity

Protect the authenticity of communications sessions.

Yes, Fully

Control Reference:

CC13.9

Comments:

No comments

Deny Network Communications By Default

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Yes, Fully

Control Reference:

CC13.10

Comments:

No comments

Prevent Split-Tunneling

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Yes, Fully

Control Reference:

CC13.11

Comments:

No comments

Terminate Network Connections

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

No

Control Reference:

CC13.12

Comments:

No comments

Session Lock

Use session lock with pattern-hiding displays to prevent access/viewing of data after a period of inactivity.

No

Control Reference:

CC13.13

Comments:

No comments

Protect Backups

Protect the confidentiality of backups at storage locations.

No

Control Reference:

CC14.19

Comments:

No comments

Remote Activation Prohibition & Use Indicators

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

No

Control Reference:

CC15.1

Comments:

No comments

Workforce Training

Implement workforce training that covers all required policies and procedures.

No

Control Reference:

CC16.1

Comments:

No comments

Awareness

Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

No

Control Reference:

CC16.2

Comments:

No comments

Insider Threat Training

No

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Control Reference:

CC16.5

Comments:

No comments

Vulnerability Scans

No

Scan for vulnerabilities and encryption status in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Control Reference:

CC17.1

Comments:

No comments

Manage Vulnerabilities

Yes, Partially

Remediate vulnerabilities in accordance with risk assessments.

Control Reference:

CC17.3

Comments:

No comments

Malicious Code Detection

Yes, Fully

Ensure that malicious code is detected.

Control Reference:

CC18.12

Comments:

No comments

Monitoring

No

Ensure that monitoring the network for unauthorized personnel, connections, devices, and software is performed.

Control Reference:

CC18.15

Comments:

No comments

Test Incident Response Plan

Yes, Partially

Ensure that the Incident Response Plan is tested.

Control Reference:

CC19.2

Comments:

No comments

Incident Documentation & Reporting

No

Ensure that events are documented and reported consistent with established criteria, including all legal and regulatory requirements.

Control Reference:

CC19.16

Comments:

No comments