About This Document:
Profile", and "Step 6: Determine, Analyze, and Prioritize Gaps" specified in the section 3.2 of the Cybersecurity Framework, as cybersecurity risk management at a company scale. It generates radar charts of the CSF Core in Function, Category, and Subcategory level.

How to Use:
- Initial Setting
Select a type of metric which a company uses, at cell B2 in "Initial Setting" sheet.
* If a company uses its own metric, define it in the sheet.

- Step 3: Create a Current Profile
organization.
* Column M can be used to indicate suggested values to be applied to each Subcategory when relevant group-wide policy and standards are fully implemented.
* Column O can be used to refer example materials to be examined when determining the value.
2. Based on your input, charts will be generated in following sheets.
"Func Lv." sheet: Function level
"Cat Lv." sheet: Category level
"Profile" sheet: Subcategory level
* Data for Pivot Table need to be refreshed/updated to generate charts.
* Values in "Func Lv." and "Cat Lv." sheets are averaged values within Function or Category.

- Step 5: Create a Target Profile and Step 6: Determine, Analyze, and Prioritize Gaps
1. Select a target value for each Subcategory in column I in "Profile" sheet based on risk assessment, security strategy, and driving forces of a company such as business requirements, business opportunities, and threats.
* If you want to input the value directly, use column J instead of column I.
2. Based on your input, charts will be generated in following sheets together with current Profile.
"Func Lv." sheet: Function level
"Cat Lv." sheet: Category level
"Profile" sheet: Subcategory level
* Data for Pivot Table need to be refreshed/updated to generate charts.
* Values in "Func Lv." and "Cat Lv." sheets are averaged values within Function or Category.

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
IDENTIFY (ID)		**ID.AM-2:** Software platforms and applications within the organization are inventoried
IDENTIFY (ID)		**ID.AM-3:** Organizational communication and data flows are mapped
IDENTIFY (ID)		**ID.AM-4:** External information systems are catalogued
IDENTIFY (ID)		**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
IDENTIFY (ID)		**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

[作業中ファイル/Work in progress]

Function	Category	Subcategory
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization’s role in the supply chain is identified and communicated
IDENTIFY (ID)		**ID.BE-2:** The organization’s place in critical infrastructure and its industry sector is identified and communicated
IDENTIFY (ID)		**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated
IDENTIFY (ID)		**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established
IDENTIFY (ID)		**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated
IDENTIFY (ID)		**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners

Function	Category	Subcategory
IDENTIFY (ID)		**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
IDENTIFY (ID)		**ID.GV-4:** Governance and risk management processes address cybersecurity risks
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented
IDENTIFY (ID)		**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources
IDENTIFY (ID)		**ID.RA-3:** Threats, both internal and external, are identified and documented
IDENTIFY (ID)		**ID.RA-4:** Potential business impacts and likelihoods are identified
IDENTIFY (ID)		**ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Function	Category	Subcategory
IDENTIFY (ID)		**ID.RA-6:** Risk responses are identified and prioritized
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders
IDENTIFY (ID)		**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed
IDENTIFY (ID)		**ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
IDENTIFY (ID)		**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

Function	Category	Subcategory
IDENTIFY (ID)		**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
IDENTIFY (ID)		**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
IDENTIFY (ID)		**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PROTECT (PR)		**PR.AC-2:** Physical access to assets is managed and protected
PROTECT (PR)		**PR.AC-3:** Remote access is managed
PROTECT (PR)		**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PROTECT (PR)		**PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation)
PROTECT (PR)		**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions

Function	Category	Subcategory
PROTECT (PR)		**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
PROTECT (PR)		**PR.AT-2:** Privileged users understand their roles and responsibilities
PROTECT (PR)		**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PROTECT (PR)		**PR.AT-4:** Senior executives understand their roles and responsibilities
PROTECT (PR)		**PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
PROTECT (PR)		**PR.DS-2:** Data-in-transit is protected
PROTECT (PR)		**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition
PROTECT (PR)		**PR.DS-4:** Adequate capacity to ensure availability is maintained
PROTECT (PR)		**PR.DS-5:** Protections against data leaks are implemented
PROTECT (PR)		**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity
PROTECT (PR)		**PR.DS-7:** The development and testing environment(s) are separate from the production environment

Function	Category	Subcategory
PROTECT (PR)		**PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
PROTECT (PR)		**PR.IP-2:** A System Development Life Cycle to manage systems is implemented
PROTECT (PR)		**PR.IP-3:** Configuration change control processes are in place
PROTECT (PR)		**PR.IP-4:** Backups of information are conducted, maintained, and tested
PROTECT (PR)		**PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met
PROTECT (PR)		**PR.IP-6:** Data is destroyed according to policy

Function	Category	Subcategory
PROTECT (PR)		**PR.IP-7:** Protection processes are improved
PROTECT (PR)		**PR.IP-8:** Effectiveness of protection technologies is shared
PROTECT (PR)		**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

Function	Category	Subcategory
PROTECT (PR)		**PR.IP-10:** Response and recovery plans are tested
PROTECT (PR)		**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
PROTECT (PR)		**PR.IP-12:** A vulnerability management plan is developed and implemented
PROTECT (PR)	**Maintenance (PR.MA)**: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PROTECT (PR)		**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
PROTECT (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PROTECT (PR)		**PR.PT-2:** Removable media is protected and its use restricted according to policy
PROTECT (PR)		**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PROTECT (PR)		**PR.PT-4:** Communications and control networks are protected

Function	Category	Subcategory
PROTECT (PR)		**PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
DETECT (DE)		**DE.AE-2:** Detected events are analyzed to understand attack targets and methods
DETECT (DE)		**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors
DETECT (DE)		**DE.AE-4:** Impact of events is determined
DETECT (DE)		**DE.AE-5:** Incident alert thresholds are established
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
DETECT (DE)		**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events
DETECT (DE)		**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events

Function	Category	Subcategory
DETECT (DE)		**DE.CM-4:** Malicious code is detected
DETECT (DE)		**DE.CM-5:** Unauthorized mobile code is detected
DETECT (DE)		**DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events
DETECT (DE)		**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed
DETECT (DE)		**DE.CM-8:** Vulnerability scans are performed
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability
DETECT (DE)		**DE.DP-2:** Detection activities comply with all applicable requirements
DETECT (DE)		**DE.DP-3:** Detection processes are tested
DETECT (DE)		**DE.DP-4:** Event detection information is communicated
DETECT (DE)		**DE.DP-5:** Detection processes are continuously improved

[作業中ファイル/Work in progress]

Function	Category	Subcategory
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident
RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed
RESPOND (RS)		**RS.CO-2:** Incidents are reported consistent with established criteria
RESPOND (RS)		**RS.CO-3:** Information is shared consistent with response plans
RESPOND (RS)		**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans

Function	Category	Subcategory
RESPOND (RS)		**RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
RESPOND (RS)		**RS.AN-2:** The impact of the incident is understood
RESPOND (RS)		**RS.AN-3:** Forensics are performed
RESPOND (RS)		**RS.AN-4:** Incidents are categorized consistent with response plans
RESPOND (RS)		**RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
RESPOND (RS)	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event,	**RS.MI-1:** Incidents are contained

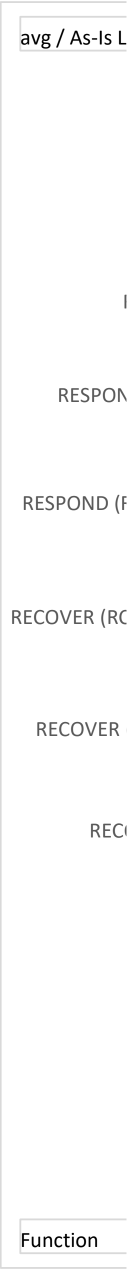
Function	Category	Subcategory
RESPOND (RS)	mitigate its effects, and resolve the incident	**RS.MI-2:** Incidents are mitigated
RESPOND (RS)		**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks
RESPOND (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned
RESPOND (RS)		**RS.IM-2:** Response strategies are updated
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident
RECOVER (RC)	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
RECOVER (RC)		**RC.IM-2:** Recovery strategies are updated
RECOVER (RC)	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed
RECOVER (RC)		**RC.CO-2:** Reputation is repaired after an incident

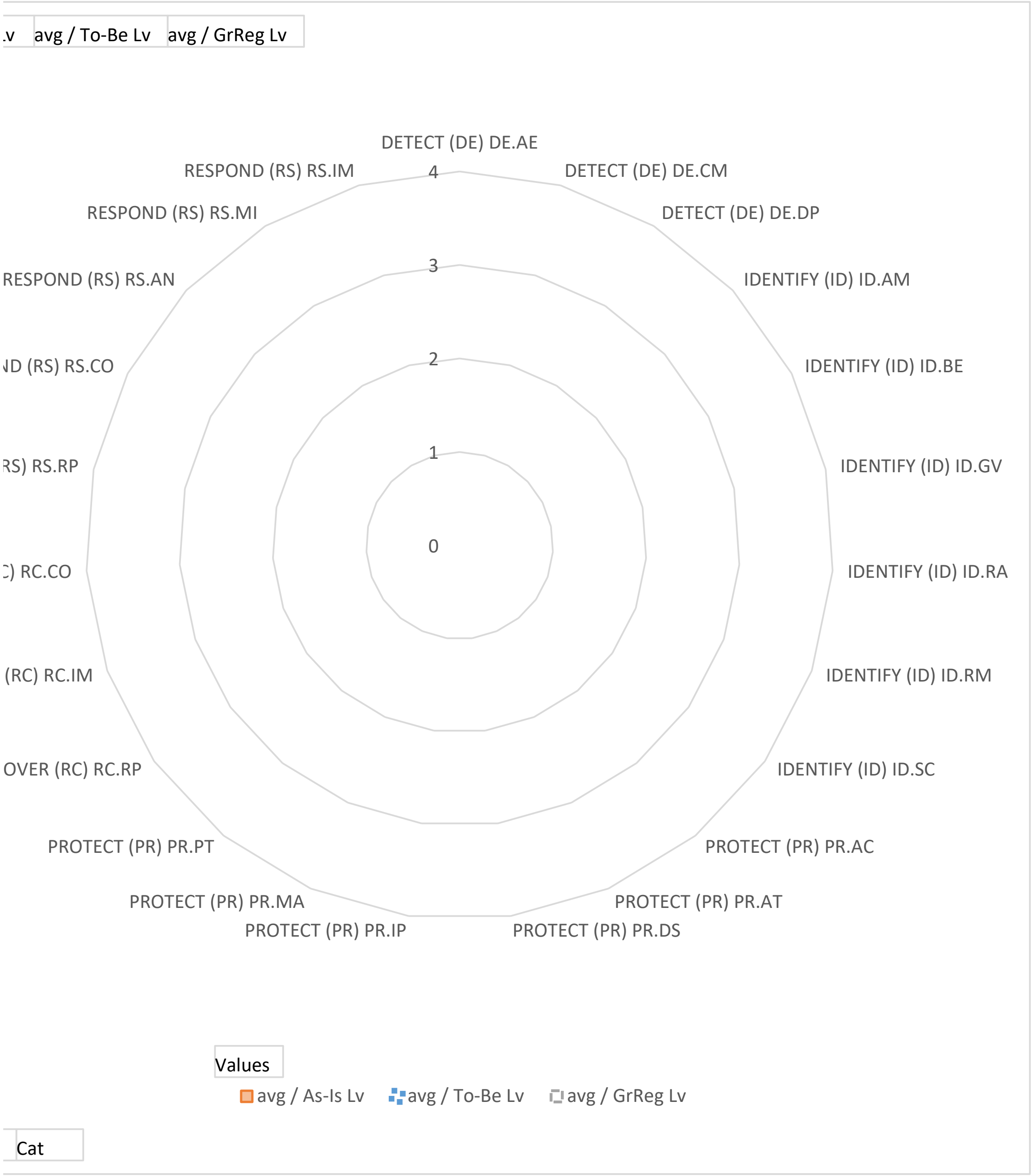
Function	Category	Subcategory
RECOVER (RC)		**RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Label	avg / As-Is Lv	avg / To-Be Lv	avg / GrReg Lv
DETECT (DE)	#DIV/0!	#DIV/0!	#DIV/0!
IDENTIFY (ID)	#DIV/0!	#DIV/0!	#VALUE!
PROTECT (PR)	#DIV/0!	#DIV/0!	#DIV/0!
RECOVER (RC)	#DIV/0!	#DIV/0!	#DIV/0!
RESPOND (RS)	#DIV/0!	#DIV/0!	#DIV/0!
Total	**#DIV/0!**	**#DIV/0!**	**#VALUE!**

avg / To-Be Lv
avg / GrReg Lv
E)
IDENTIFY (ID)
PROTECT (PR)
RECOVER (RC)
RESPOND (RS)
Values
🟧 avg / As-Is Lv
🟦 avg / To-Be Lv
⬜ avg / GrReg Lv

Label	avg / As-Is Lv	avg / To-Be Lv	avg / GrReg Lv
DETECT (DE)			
DE.AE	#DIV/0!	#DIV/0!	#DIV/0!
DE.CM	#DIV/0!	#DIV/0!	#DIV/0!
DE.DP	#DIV/0!	#DIV/0!	#DIV/0!
IDENTIFY (ID)			
ID.AM	#DIV/0!	#DIV/0!	#VALUE!
ID.BE	#DIV/0!	#DIV/0!	#DIV/0!
ID.GV	#DIV/0!	#DIV/0!	#DIV/0!
ID.RA	#DIV/0!	#DIV/0!	#DIV/0!
ID.RM	#DIV/0!	#DIV/0!	#DIV/0!
ID.SC	#DIV/0!	#DIV/0!	#DIV/0!
PROTECT (PR)			
PR.AC	#DIV/0!	#DIV/0!	#DIV/0!
PR.AT	#DIV/0!	#DIV/0!	#DIV/0!
PR.DS	#DIV/0!	#DIV/0!	#DIV/0!
PR.IP	#DIV/0!	#DIV/0!	#DIV/0!
PR.MA	#DIV/0!	#DIV/0!	#DIV/0!
PR.PT	#DIV/0!	#DIV/0!	#DIV/0!
RECOVER (RC)			
RC.RP	#DIV/0!	#DIV/0!	#DIV/0!
RC.IM	#DIV/0!	#DIV/0!	#DIV/0!
RC.CO	#DIV/0!	#DIV/0!	#DIV/0!
RESPOND (RS)			
RS.RP	#DIV/0!	#DIV/0!	#DIV/0!
RS.CO	#DIV/0!	#DIV/0!	#DIV/0!
RS.AN	#DIV/0!	#DIV/0!	#DIV/0!
RS.MI	#DIV/0!	#DIV/0!	#DIV/0!
RS.IM	#DIV/0!	#DIV/0!	#DIV/0!
Total	**#DIV/0!**	**#DIV/0!**	**#VALUE!**




.v
avg / To-Be Lv
avg / GrReg Lv
DETECT (DE) DE.AE
DETECT (DE) DE.CM
DETECT (DE) DE.DP
IDENTIFY (ID) ID.AM
IDENTIFY (ID) ID.BE
IDENTIFY (ID) ID.GV
IDENTIFY (ID) ID.RA
IDENTIFY (ID) ID.RM
IDENTIFY (ID) ID.SC
PROTECT (PR) PR.AC
PROTECT (PR) PR.AT
PROTECT (PR) PR.DS
PROTECT (PR) PR.IP
PROTECT (PR) PR.MA
PROTECT (PR) PR.PT
OVER (RC) RC.RP
(RC) RC.IM
) RC.CO
RS) RS.RP
ND (RS) RS.CO
RESPOND (RS) RS.AN
RESPOND (RS) RS.MI
RESPOND (RS) RS.IM
4
3
2
1
0
Values
🟧 avg / As-Is Lv
▨ avg / To-Be Lv
□ avg / GrReg Lv
Cat

Own definition <- Select metric definition

1: A relevant organizational rule is not defined, but a subcategory (outcome) is implemented p

1.5: A relevant organizational rule is defined, and a subcategory (outcome) is implemented pa

2: A relevant organizational rule is defined, and a subcategory (outcome) is implemented base

2.5: A relevant organizational rule requiring continuous improvement is defined, and a subcate

3: A relevant organizational rule requiring continuous improvement is defined, and a subcateg

3.5: A relevant organizational rule requiring continuous improvement and timely adoption of t

4: A relevant organizational rule requiring continuous improvement and timely adoption of the

Own definition ↓ Modify definition below if a company uses its own definition.

Level	definition
1	A relevant organizational rule is not defined, but a subcategory (outcome) is implemented partially.
1.5	A relevant organizational rule is defined, and a subcategory (outcome) is implemented partially based on it.
2	A relevant organizational rule is defined, and a subcategory (outcome) is implemented based on it.
2.5	A relevant organizational rule requiring continuous improvement is defined, and a subcategory (outcome) is implemented partially based on it.
3	A relevant organizational rule requiring continuous improvement is defined, and a subcategory (outcome) is implemented based on it.
3.5	A relevant organizational rule requiring continuous improvement and timely adoption of the latest information is defined, and a subcategory (outcome) is implemented partially based on it.
4	A relevant organizational rule requiring continuous improvement and timely adoption of the latest information is defined, and a subcategory (outcome) is implemented based on it.

Holdings de

Level
1
1.5
2
2.5
3
3.5
4