

Promotion of Critical Infrastructure Protection through Public-Private Partnership

- Based on the concept of **mission assurance**, ensure the **safe and continuous provision of critical infrastructure services**
- Promote **initiatives to ensure cybersecurity of critical infrastructure through integrated efforts by the public and private sectors**

Comprehensive Coordination by the NCO

Competent Ministries and Agencies for Critical Infrastructure

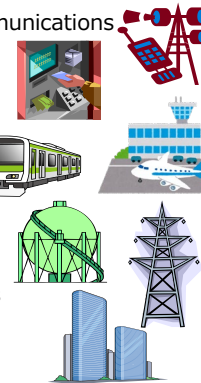
- Financial Service Agency
[Financial Services]
- Ministry of Internal Affairs and Communications
[Information and Communications, Administrative Services, Postal Services]
- Ministry of Health, Labor and Welfare
[Healthcare]
- Ministry of Economy, Trade and Industry
[Electricity, Gas, Chemicals, Credit, Petroleum]
- Ministry of Land, Infrastructure and Transport and Tourism
[Aviation, Airports, Railways, Water Supply, Logistics, Ports and Harbors]



Related Organizations, etc.

Critical Infrastructure (16 Sectors)

- Information and Communications
- Financial Services
- Aviation
- Airports
- Railways
- Electricity
- Gas
- Administrative Services



- Healthcare
- Water Supply
- Logistics
- Chemicals
- Credit
- Petroleum
- Ports and Harbors
- Postal Services



Key Initiatives in the Action Plan for Cybersecurity of Critical Infrastructure

Strengthening Incident Response Systems



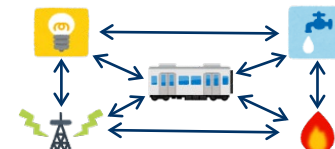
Development and Dissemination of Safety Standards, etc.



Strengthening Information Sharing Systems



Utilization of Risk Management



Strengthening the Protection Foundation



1. Purpose of CIP

Based on the concept of mission assurance, the purpose of CI protection (CIP) is to maintain safe and continuous provision of CISs by ensuring resilience and preventing serious impact on national life and socioeconomic activities from the dual aspects of below;

- Limit risk to acceptable levels taking the view that natural disasters, mismanagement, cyberattacks, and changes in the environment surrounding CI constitute risks that make the continuous provision of CISs uncertain.
- Take appropriate action in the event of outages and ensure rapid restoration of services in terms of preparing for CISs outages.

2. Responsibilities of stakeholders

- Responsibilities of stakeholders are based on the Basic Act on Cybersecurity (Act No. 104 of 2014).
- The national government is responsible for formulating and implementing comprehensive cybersecurity policies.
- Local governments bear the responsibility to formulate and implement independent cybersecurity policies.
- CI operators (excl. related entities) bear the responsibility to deepen their interest in and understanding of the importance of cybersecurity and to endeavor independently and actively to ensure cybersecurity, in order to stably and properly provide its services.
- Cyberspace-related business entities and other business entities shall endeavor independently and actively to ensure cybersecurity in the course of their business activities.

3. Basic concept

- In response to the increasingly sophisticated and complex usage of systems and the rapidly increasing threats in cyberspace, CI operators will further promote organization-wide responses, involving top management, CISOs, strategic management, and system personnel. Particular measures will be taken towards promoting cybersecurity as an important priority for management.
- CI operators will clarify the specific characteristics of their organization and implement the most appropriate CIP policies by utilizing risk management that organically combines the perspectives of all organizational levels, from top management through to system personnel.
- In order to respond precisely to changes to threats relating to CI, a comprehensive response is implemented capable of anticipating future changes in the environment, including in the supply chain, etc.

4. Strengthening incident response systems

- Strengthen incident response systems through a combination of preemptive risk management and crisis management.
- Clarify the relationship between top management and experts for ensuring organizational cybersecurity.
- Based on the definition stipulated in Article 2 of the Basic Act on Cybersecurity, to ensure cybersecurity develop and operate an incident response systems capable of responding not only to external attacks, but also to events related to system procurement, design, and operation.

Critical infrastructure operators, etc. will **strengthen their incident response systems through close mutual cooperation between the public and private sectors**, after making their **organization-wide efforts** to ensure cybersecurity.

Key points of activities

- ✓ Strengthening incident response systems as part of the organizational governance
- ✓ Comprehensive response, including supply chain

Activities during this Action Plan term

(1) Incident response systems as part of organizational governance

- Promote the strengthening of incident response systems of the entire organization, including top management, CISO, strategic management, and system personnel, etc., and operators involved in the supply chain, etc.

(2) Activities to strengthen incident response systems

- Promote effective activities for BCP/IT-BCP, CSIRT, audit system, etc. to strengthen incident response systems

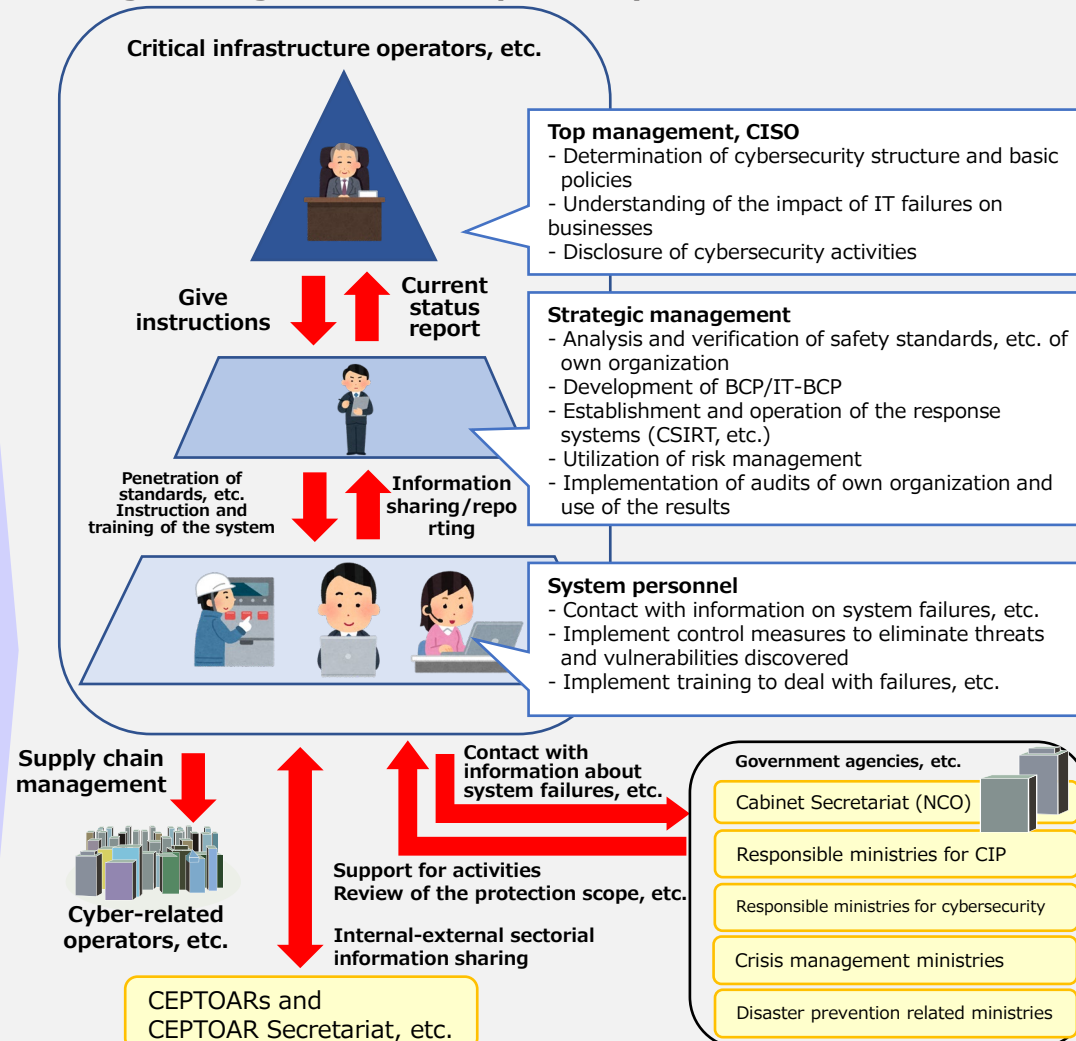
(3) Integrated public-private efforts to strengthen incident response systems

- Consider integrated public-private efforts with close mutual cooperation between the government and critical infrastructure operators, etc.

(4) Review of the protection scope of CI

- Ensure "protection as plane" including the supply chain and from a security perspective in order to respond to changes in the environment

Strengthening Incident Response Systems



In order to implement the most appropriate protection measures for own organizations, **promote activities for the maintenance and promotion of the "safety standards, etc." by the stakeholders such as critical infrastructure operators.**

* Safety standards, etc.: General term for relevant laws, industry standards/guidelines, internal regulations, etc.

Key points of activities

- ✓ Make continuous improvement and dissemination of safety standards, etc. based on the Common Cybersecurity Standards for Critical Infrastructure and the Guidelines for Establishing Safety Standards, etc. for Cybersecurity of Critical Infrastructure

Activities during this Action Plan term

(1) Continuous improvement of the safety standards

- Identification of challenges through the operation of cybersecurity initiatives, internal and external audits, analyses of changes in the cybersecurity environment, exercises and training, and responses to service disruptions, and improvement of safety standards, etc. through risk assessment, based on knowledge and lessons learned from critical infrastructure measures

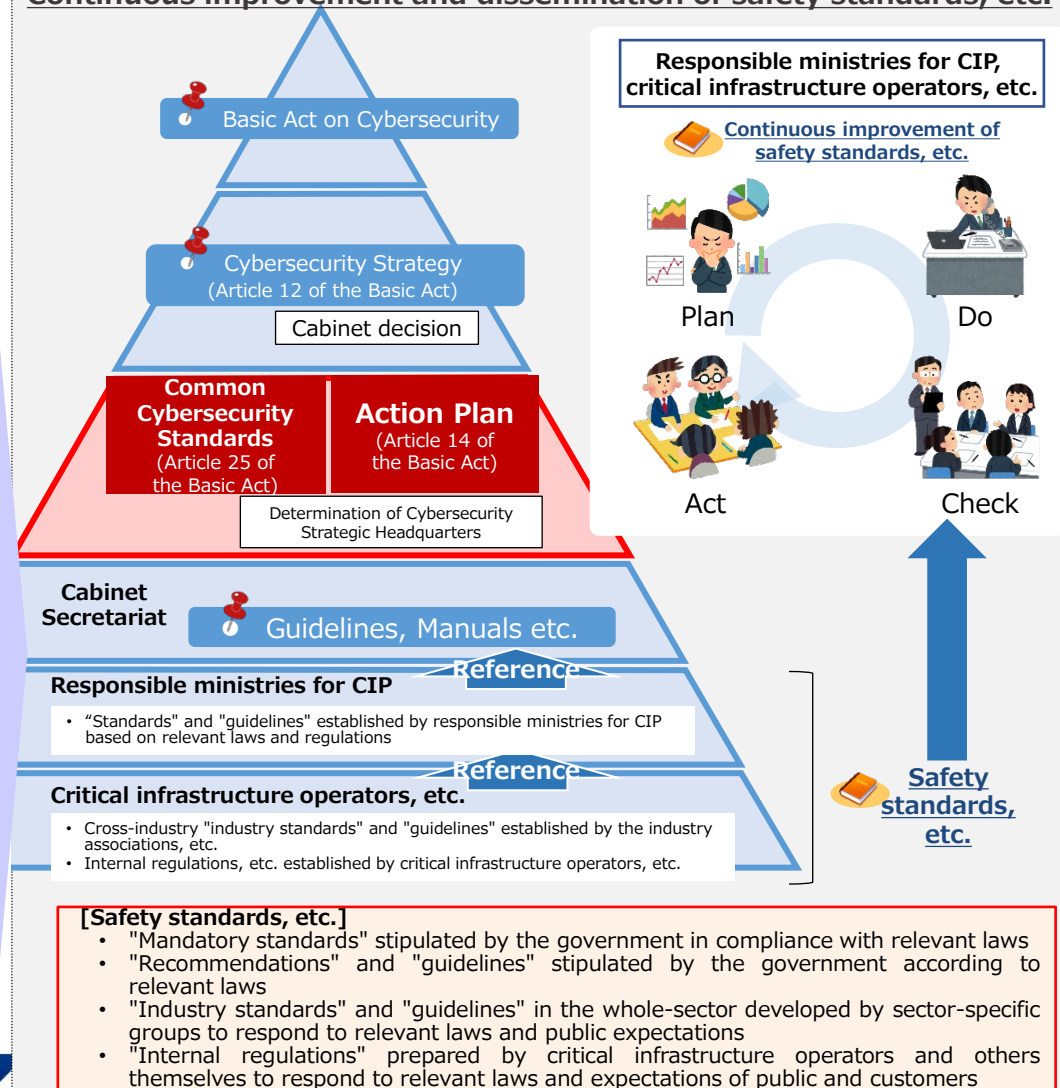
(2) Dissemination of the safety standards

- Detailed assessment of the effectiveness of incident response systems through surveys and analyses of the development status of safety standards and of activities and measures being implemented to ensure cybersecurity

(3) Clarification of documentation relating to the safety standards

- Listing of documents and clarification of relationships between documents to promote understanding of Common Cybersecurity Standards for Critical Infrastructure, safety standards, etc.

Continuous improvement and dissemination of safety standards, etc.



Work to enhance public-private and internal-external sectoral information sharing systems further so that individual critical infrastructure operators, etc. can respond to cybersecurity trends that change on a daily basis.

Key points of activities

- ✓ Develop and disseminate the information sharing systems built under the previous policies.
- ✓ Activate voluntary efforts by critical infrastructure operators, etc.

Activities during this Action Plan term

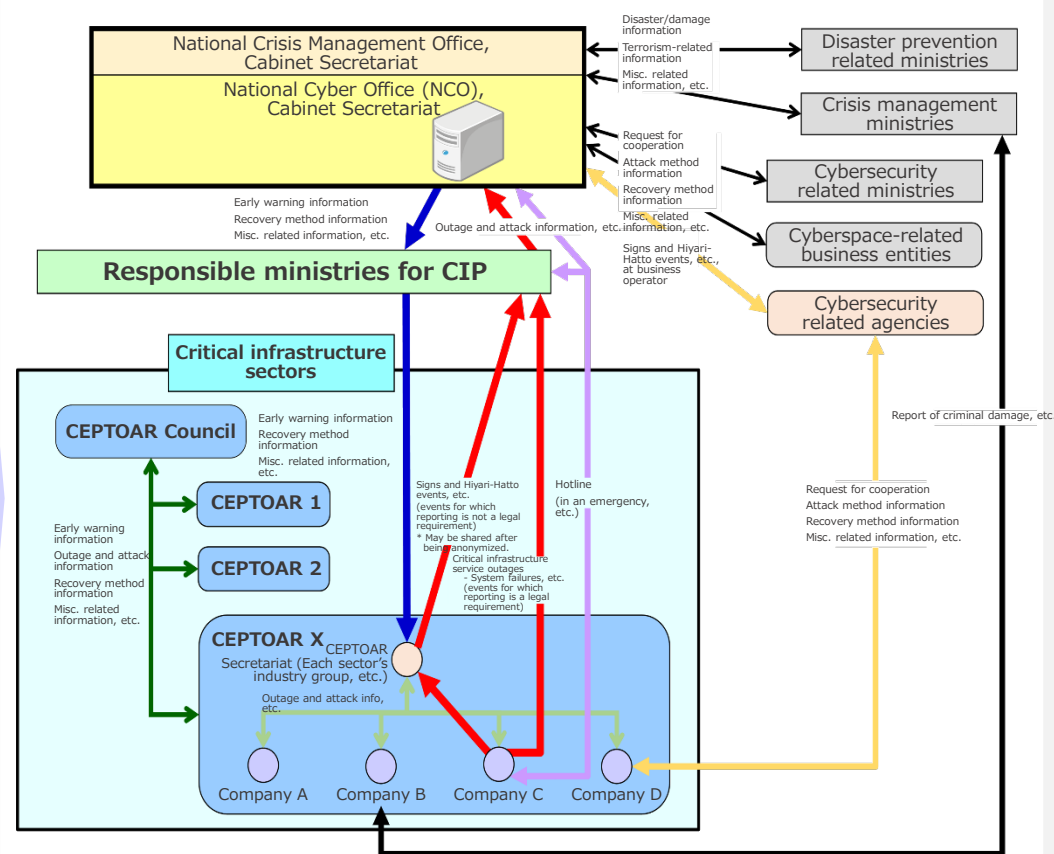
(1) Further promotion of information sharing

- Proactive utilization for risk management of shared information
- Aggregation, analysis and sharing of information related to critical infrastructure service outages and threat and vulnerability information
- Clarification of what information should be shared (Clarify that not only information systems but also control systems and IoT systems should be covered, and so on.)
- Timely and appropriate review in the event of environmental changes, etc.

(2) Promotion of CI operators' activities

- Establishment and enhancement of the incident response systems under the leadership of top management
- Further enhancement of information sharing within and between CEPTOARs
- Promotion of participation in ISACs and information sharing among ISACs
- Implementation of CEPTOAR training in a more realistic manner

Information Sharing Systems in the Critical Infrastructure



Aiming to ensure resilience in the continual provision of critical infrastructure services, **promote continuous efforts in repeated PDCA cycles of protection measures optimized to individual organizations.**

Key points of activities

- ✓ Realization of protection measures optimized to individual organizations
- ✓ Identification of new risks and risk sources due to environmental changes
- ✓ Analysis of interdependency among critical infrastructure sectors

Activities during this Action Plan term

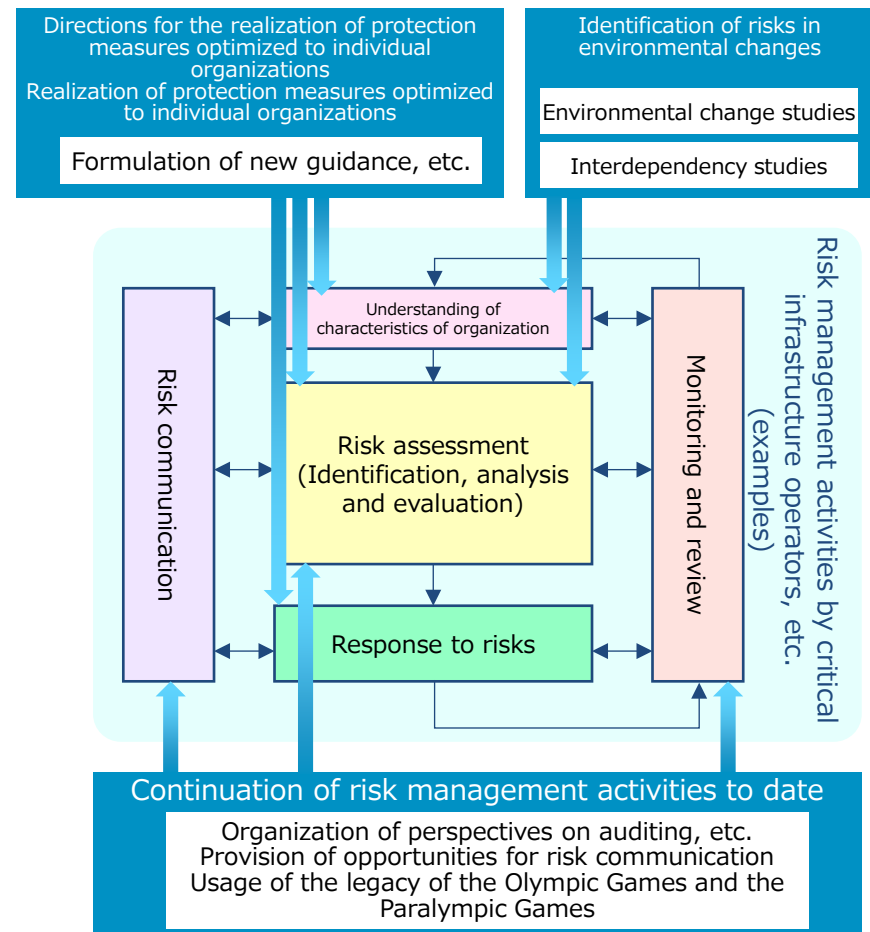
(1) Promotion of risk management

- Clarification of the profile of own organization and promotion of efforts to realize protection measures optimized to individual organizations
- Review of the effective measures and usage of existing standards, review of manuals and development of new guidance, etc.

(2) Studies and analysis of risks

- Implementation of environmental change studies to address risks due to the transformation of cyberspace as a result of the advancement of DX with digitalization, etc.
- Implementation of interdependency studies of which other critical infrastructure sectors would be affected in the event of a critical infrastructure service outage

Utilization of Risk Management



In order to strengthen the protection foundation, **promote activities which support the entirety of the policy**, such as verification of the effectiveness of the incident response systems, human resources development, cooperation with related agencies, international cooperation, public relations activities.

Key points of activities

- ✓ Implementation of effectiveness verification of incident response systems
- ✓ Development of human resources not only in the IT sector but also in a wide range of other sectors
- ✓ Information dissemination through effective PR channels, etc.

Activities during this Action Plan term

(1) Verification of effectiveness of incident response systems

- Verification of incident response systems through cross-sectoral exercise
- Improvement of incident response systems by using the issues from the exercise

(2) Promotion of the development of human resources

- Develop strategic management personnel to work closely with top management
- Raise awareness throughout the organization, not just in the IT department

(3) Promotion of international cooperation

- Promote multifaceted international cooperation through various governmental, industry, and multi-stakeholder frameworks

(4) Strengthening of cooperation with the National Police Agency and the Digital Agency

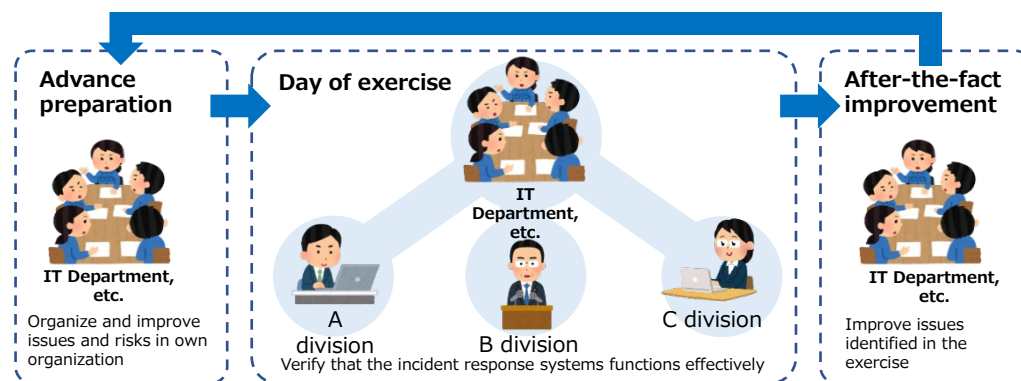
- Promote overall security by raising awareness of cybercrime and new technologies associated with DX

(5) Promotion of public relations activities

- Making the framework and activities of the action plan easy to understand for the public
- Maintenance of relevant documents and standards

Activities for strengthening the protection foundation

Verification of effectiveness of incident response systems



Development of Human resources



- Develop strategic management
- Raise awareness throughout the organization

International cooperation



bilateral or multilateral cooperation

Strengthening of cooperation with the National Police Agency and the Digital Agency



警察庁
National Police Agency

デジタル庁

- Reporting cybercrimes to the police, etc.
- Securing of cyberspace security through raising the awareness for new technologies associated with DX

Public relations activities



Web



Lecture



SNS



Newsletter

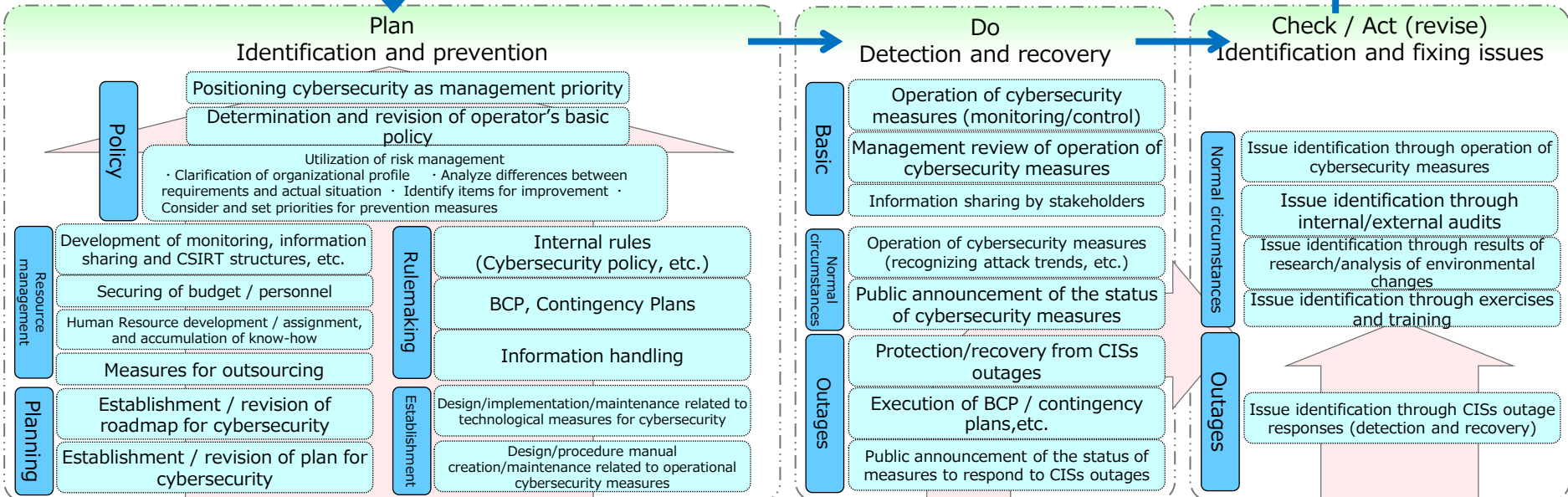
Dissemination through website, social media, newsletter, lectures, etc.

"Critical Infrastructure Operator Measure Examples" and "Government Activities"

8

Understanding of the responsibilities of stakeholders under the Basic Act on Cybersecurity

Critical infrastructure operator measure examples



Government activities

