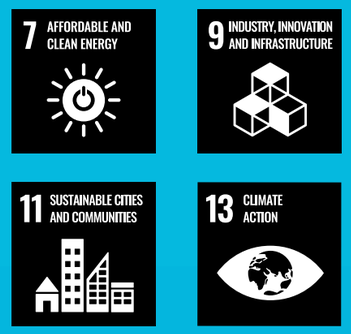
4 SUSTAINABILITY RISKS AND OPPORTUNITIES

CHT places emphasis on the control of the corporate operation and sustainability risk. In 2016, the Company established a Risk Management Committee with the President as convener and high rank managers as members. The committee supervises risk management throughout the organization and is responsible for prioritizing identified risks, formulating response strategies to key risk issues, and reporting to the board of directors when deemed necessary. Through control of the mechanism at each level, potential risks and loss to the Company can be minimized.

The SDGs CHT contributes to in this chapter:



TCFD *The **first** telecom operator in the world to pass "**TCFD Conformity Check**" with **the highest grade obtained for 3 consecutive years**.*

*CHT is actively looking into the development of **renewable energy**, self-built or **for sale soar energy installation.***

*Our "**Risk Management Committee**" adopts Enterprise Risk Management (ERM) software to govern every business decision made by our employees.*

AIoT *The development of the Artificial Intelligence will popularize edge computing, IoT drones, AR and VR. These emerging industries will **propel the development of hardware and operating systems.***

*Based on NIST's Cybersecurity Framework (CSF) and domestic and international standards and regulations, CHT established the **"Chunghwa Telecom Cybersecurity and Privacy Protection Framework."***

CHT Risk Management Organization Structure

Aspects	Description
Organizational Aspect	· "Risk Management Committee" was established in 2016, which convenes committee meeting regularly, presents execution report monthly, reports the operation to the Board of Directors quarterly, and reports to the Audit Committee and Board of Directors on material risk events.
Strategic Aspect	· Risk policies and framework stipulated by the Board of Directors. · "Risk Management Policy" and "Directions Governing the Risk Management Operation" as the bases for all personnel's reference in conducting business.
Management	· The Enterprise Risk Management (ERM) system was established for the regular control of the risks, and we track it on a rolling basis.
Assessment Tool	· We use the Risk Analysis Matrix as our assessment tool to assess operational, strategic, compliance and reporting risks, etc. · For the major operational items and relative ESG issues, including climate-related risks, we enhance the performance of sensitivity analysis and the stress test. · Pursuant to Recommendations of the Task Force on Climate-related Financial Disclosures (referred to as "TCFD Framework" hereinafter), we analyzed the scope of operation, upstream and downstream, as well as the climate-related risks and opportunities throughout the life cycles of assets in the short-, mid-, and long-terms.
Audit Aspect	· Risk Management Committee promotes implementation of risk management efforts of the Company and evaluates performances in risk management. · The Audit Department reviews the risks and reports to the Board of Directors. · The management and control results are incorporated as part of the performance appraisal of respective institutions.
Feedback and Improvement	· Risk status is followed up monthly and reported to the Risk Management Committee convener and the Audit Department. · The Risk Management Committee (in addition to the committee members, the Chief Audit Executive is present) convenes regularly as well as reports to the Audit Committee and the Board of Directors. · The Committee improves the current risk management mechanism based on Risk Management Committee, Audit Committee and Board of Directors' decision to ensure the process is up to date and satisfies the operational need.
Implementation Results in 2022	· **3 meeting were convened with focuses on the enterprise-level risks tied with the objectives in the business plans and deliberations on directions of material risk topics.** · **Reported to the Audit Committee twice and to the Board of Directors four times on the implementation of risk management.**

* For more information about Risk Management, please refer to:

Emerging Risks

CHT continues with advanced technological research and development to take advantage of many business opportunities in this digital convergence era and reduce operational risk. We absorb, cultivate and make good use of excellent available talent to integrate Internet and marketing resources.

We cooperate closely with our strategic partners in the launch of new services and products that satisfy our customers. We have become the Digital Economy Motivator and the Creative Industry Pilot, and we create values for clients, shareholders, employees and society.

Risk Factor

Dwindled advantage in the mobile services market due to the merger of competitors

Potential Influences ▮ Obstacles

Increased bandwidth and user population of competitors that leads to impact to our mobile market share

Countermeasures ▮ Risk Avoidance and Opportunity Seizure

· Strengthen 4G/5G construction, introduce 5G dual band service, and new features, including introduction of 5G NR CA, addition of 4G stations, and ongoing improvement to network coverage and capacity.
· Establish the network advantage of "Always Broadband Connected" with triple networks of mobile networks, optical networks, and Wi-Fi services combined to boost the QoE of users.

Risk Factor

Twists in the energy transition for the net-zero emissions policy

Potential Influences ▮ Obstacles

It affects the power supply stability

Countermeasures ▮ Risk Avoidance and Opportunity Seizure

· Strengthen the resiliency of networks to ensure business continuity, e.g. strengthen the emergency backup capacity of networks and IDCs, request Taipower to adopt dual-feeder power supply for critical IDCs, increase the emergency power generation units and batteries installed, phase out old energy-consuming equipment, and introduce low-carbon network equipment, etc.

Risk Factor

Impediment to achievement of the net-zero goal due to the short supply of renewable energy

Potential Influences ▮ Obstacles

Potential impact on the willingness of customers, and even the international investors and ratings, due to failure of IDCs to attain the carbon reduction target

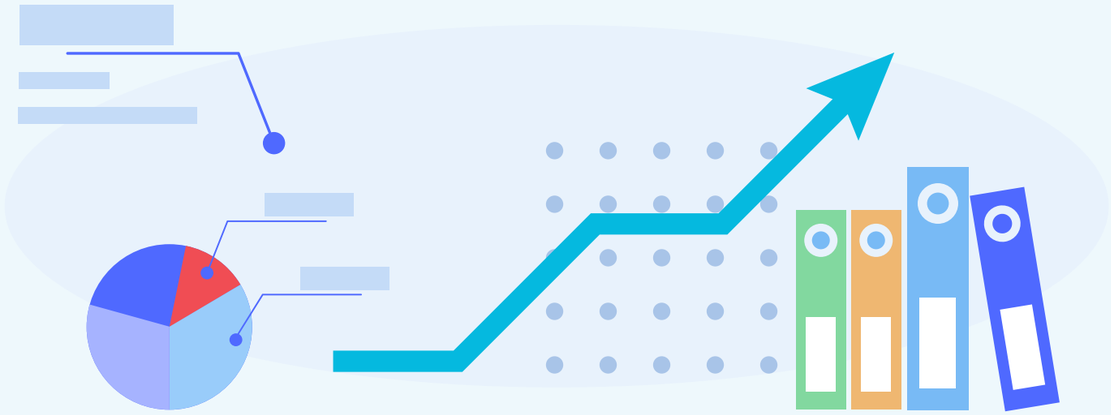
Countermeasures ▮ Risk Avoidance and Opportunity Seizure

· Actively explore for stable and sufficient supplies of renewable energy, obtain the supply of solar power and onshore wind power first through short-term contracts to wheel power to IDCs for use, and seek signing of long-term CPPA depending on the progress of the government's development in the sector of offshore wind power.
· Preemptively enter the energy transition industry to reduce risks.

Emerging Opportunities

The 5G+AIoT technology will drive intelligent technological applications and push corporations in Taiwan to move their business emphasis. With the advent of Industry 4.0 and the rapid emergence of new online applications, cybersecurity specialists are issuing warnings regarding the looming threat of multimodal, multifaceted attacks. However, this also creates an opportunity for companies that offer an integrated cybersecurity service package. The government has classified information security as a matter of national security, including it as part of the national defense industry in the 5+2 New and Innovative Industries Policy.

CHT spares no effort in the refinement of cybersecurity technology. In 2017, CHT founded CHT Security, a subsidiary with all 5 service items rated as "A" in the Cyber Security Service Provider Assessment of the Executive Yuan for 4 consecutive years. Aside from assisting in the regional joint defense of cybersecurity for 15 counties/cities domestically, it further supports numerous important entities in the public sector, finance, high-tech manufacturing, medicine, critical infrastructure, etc. in terms of cybersecurity check and protection.



Opportunity Factor

Information Security Management

Potential Business Opportunity

- Popularization of emerging technological applications as well as diversified attacks by hackers boost the challenge of protection against cybersecurity threat while create new opportunities in the cybersecurity area.
- The FSC promulgated "Financial Cyber Security Action Plan" to drive the demands for cybersecurity protection, monitoring, and joint defense in the financial sector.
- The Executive Yuan announced the Cybersecurity Industry Development Action Plan. The gross output of the industry is expected to exceed NT$ 78 billion dollars by 2025.
- Gartner pointed out that the global cybersecurity market accounted for approximately 3.32% of the global IT expenditures and rising.

Countermeasures ■ Risk Avoidance and Opportunity Seizure

- As a managed security service provider (MSSP), we dedicated to the provision of a wide range of cybersecurity solutions. With the strategy of extensive alliance ,become the leader in the cybersecurity industrial chain integration.
- Create a low-burden, high-standard Advanced Networks Defense system (ANDs) for enterprises, complete the section 2 expansion of DDoS protection, and improve the IPS2.0 intrusion protection quality.
- The Digital Forensics and Cyber Security Testing Center of the subsidiary, CHT Security Co., Ltd., has been certified with the testing and certification of IoT devices and IEC 62443 CB TESTING LABORATORY (CBTL) in order to build a safer OT environment.

Opportunity Factor

Development of 5G

Potential Business Opportunity

Forecast from Qualcomm "The 5G Economy" shows that 5G technology will result in an output of US$ 134 billion to the companies in Taiwan in 2035.

Countermeasures ■ Risk Avoidance and Opportunity Seizure

- Launching "Taiwan 5G Industry Development Alliance - CHT leading team" to jointly promote 5G development, establish robust 5G operations, research and development, manufacturing, and enhance our 5G sales force.
- Participate in the Asia Silicon Valley Development Plan of the National Development Council to assist in promoting the domestically produced equipment in global market.

AIoT

Opportunity Factor

AIoT

Potential Business Opportunity

- Following the ease-up of the global pandemic and gradual recovery of production demand in the supply chain, the output value of IoT in Taiwan has exceeded NT$2 trillion in 2022.
- New application opportunities, including net-zero carbon emissions, metaverse, electric vehicles, etc., present business opportunities for the development of the IoT industry.

Countermeasures ■ Risk Avoidance and Opportunity Seizure

- In connection with 5G+AIoT innovative technology, the five focused areas, i.e. Smart Building, Smart Transportation, Smart Security, Smart Energy, and Smart Medicine, are developed together with the industry to build smart IoT solutions and services that are more convenient and safer for the government and enterprises.
- 5G+AIoT continues to march towards the corporate target of NT$10 billion revenue by 2025.

Opportunity Factor

Climate Change (low carbon products and services)

Potential Business Opportunity

- The World Economic Forum (WEF) predicted that of the potential risks in the next decade, four out of the top five risks are environmental issues, especially the "extreme weather."
- Businesses around the globe are investing in low carbon emission infrastructure, including green energy, electric automobiles, and smart cities to reduce reliance on electricity.
- The bonds issued by green enterprises worldwide in 2021 were up to $416.5 billions' worth, accounting for 3.51% of the corporate bonds issued globally and rising.

Countermeasures ■ Risk Avoidance and Opportunity Seizure

- Green Product and Service Program — we provide energy-saving technology and services.
- We reduce carbon footprints through innovative green services, cloud products, and other technologies.
- We are building a cloud service platform that enables clients to access real time data regarding their energy usage and equipment status so that failures can be predicted and prevented.
- The sustainable development bond was issued. The fund raised shall be directed to green buildings and comprehensive VoIP for telephone networks , so as to realize the carbon reduction for all via technology.

Climate Change Risks and Opportunities

Chunghwa Telecom builds a systematic and organized corporate governance structure to ensure that climate change related challenges are incorporated into the Company's annual strategy in real time and that relevant projects are implemented.

The Supervisory Responsibility of the Board of Directors

The climate change-related risks and opportunities are managed through the dual mechanisms of Sustainable Development Committee and Risk Management Committee. In addition, with the existing internal control and risk management mechanisms combined, the links between the climate change topics and the Board of Directors' responsibility in the oversight thereof is strengthened through the report to the Board of Directors quarterly.

Task Force on Climate-related Financial Disclosures (TCFD)

Chunghwa Telecom is the first telecom company in Taiwan to sign on as supporter of the Task Force on Climate-related Financial Disclosures (TCFD) initiative. The Task Force on Climate-related Financial Disclosures (hereinafter as "TCFD") has been introduced in 2019 to conduct analyses of climate risks and opportunities so as to promote works of climate change mitigation and adaptation for an ongoing reduction of operational risks for the Company and drive the low-carbon transformation in the industrial chain. In 2023, CHT was certified to the highest grade of TCFD Conformity Check for 3 consecutive years.

* For Chunghwa Telecom TCFD report, please refer to:

For Climate-related Information of TWSE and TPEx Listed Companies, please refer to p.167 of our 2022 ESG report.

The Role of Management

The "Environmental Group" is set up under the CHT Sustainable Development Committee. Pursuant to the ESG vision and carbon management strategies laid out by the Board of Directors and the Sustainable Development Committee, in line with the needs of international institutional investors, rating agencies, and key stakeholders, it plans, enforces, and manages execution of various climate change and carbon management action plans. The relevant mechanisms include:

Target Setting:

Target setting for the net-zero emissions, GHG reductions, and climate resilience improvement of CHT.

Strategic Planning:

Strengthening the carbon management competencies of the Company and its supply chain with mitigation and adaptation at the core, along with improvement of climate resilience of the telecom infrastructure and communication equipment, to ensure business continuity.

Solutions:

Proposal of innovative solutions to reduce GHG emissions from itself and the industrial chain; planning and execution of "Action Plans for Adaptation to Climate Change in the next 20 Years for Chunghwa Telecom Communication Networks" to deploy climate change adaptation actions.

CHT Climate Change Strategies

Mitigation

Attainment of net-zero emissions is the foremost mission, along with facilitation to partners, upstream and downstream, to collectively realize the target of 1.5°C set in the Paris Agreement.

Adaptation

Improvement of the climate resilience for the infrastructure and communication equipment of the Company is the foremost mission to ensure business continuity for the Company.

To analyze the future impacts of climate change on the Company, we employed the TCFD structure, setting a baseline scenario and a 1.5°C scenario to identify and analyze the short-, medium-, and long-term climate risks and opportunities in the business scope of the Company, the upstream and the downstream, and the entire life cycle of assets. IEA STEPS (baseline scenario) and IEA NZE (1.5°C scenario) are employed as the climate scenarios for climate mitigation strategies (transition risks). IPCC RCP 8.5 (baseline scenario) and IPCC RCP 2.6 (1.5°C scenario) are employed as the climate scenarios for climate adaptation strategies (physical risks).

Notes: 1. STEPs: Stated Policies Scenario; 2. NZE: Net Zero Emissions; 3. RCP: Representative Concentration Pathway

Climate Change Scenarios for "Mitigation and Adaptation"

Mitigation

IEA STEPs

- In this scenario, the government sets a net-zero emission target for 2050, with the base year of 2005. The carbon reduction target: 10% reduction in 2025, 24% ± 1% reduction in 2030, net-zero emissions in 2050, and other policies unchanged.
- The parameters we use are the reduced input costs for Scope 1 and 2 and assume the financial impact of a scenario where the achievement of net-zero emissions is mandatory in the future.

IEA NZE

- In this scenario, the government targets for net-zero emissions by 2050. With the assumption that the government amends the law and sets the base year as 2020, the carbon reduction target moves up to a 21% reduction in 2025, a 42% reduction in 2030, and net-zero emissions in 2050, along with the policies strengthened.
- The parameters we use are the reduced input costs for Scope 1 and 2 and assume the financial impact of a scenario where the achievement of net-zero emissions is mandatory in the future.

Adaptation

IPCC RCP 2.6

- In this scenario, according to the analysis of the "Taiwan Climate Change Projection Information and Adaptation Knowledge Platform (TCCIP)" of the Ministry of Science and Technology for extreme weather events (e.g. typhoons and heavy rains), the number of typhoons that will invade Taiwan in the future will decrease, but the percentage of strong typhoons will increase, the precipitation intensity will rise, and the frequency and intensity of torrential rain shall remain on the rise.
- The parameter we use is operating costs, with the assumption that typhoon is to render loss of equipment, which will incur costs in repairment.

IPCC RCP 8.5

- In this scenario, countries do not take any measures, leading to ever-rising temperatures, exacerbating extreme weather events.
- The parameter we use is operating costs, with the assumption that typhoon is to render loss of equipment, which will incur costs in repairment.

Climate Risks & Opportunities Assessment

We classified risks related to the industry as transition risks and physical risks and established the list of topics of risks and opportunities according to TCFD Directions. The risks fall into categories of policy and legal, technology, market, reputation of transition risks; acute and chronic of physical risks. Meanwhile, the opportunities are divided into resource efficiency, energy source, products/services, market, and resilience. Hence, we performed the identification and assessment process with the climate change risks and opportunities. The process is performed on a yearly basis in principle, covering us and the upstream/downstream as well as 100% the existing and new operating sites and communication equipment around Taiwan.

Risks / Opportunities	Category	Time			Issues
		short-term	Medium-term	long-term	
Transition risk	Policy and Legal	✓	✓	✓	· Increased costs for GHG emissions due to the national policy of Net Zero Emissions · Necessity in the investment in renewable energy owing to national renewable energy policy · Increased operating costs arising from addition of other sustainability-related laws and regulations
	Technology	✓	✓	✓	· Failure in new technology investment (e.g. a technology developed not meeting the low-carbon benefits, rendering failure of the new technology invested) · Missed involvement in the low-carbon R&D trend for failure of investment in the low-carbon transformation technologies
	Market	✓	✓	✓	· Changes in customer behaviors (e.g. elevated consumer awareness for climate change or shift in product/service demands)
	Reputation		✓	✓	· Impact to reputation from litigation risks · Impact to reputation due to carbon reduction performance of suppliers not as expected
Physical risk	Acute	✓	✓		· Damage to facility/equipment due to increased severity of extreme weather events like typhoon or flood · Product supply disruption/delay arising from impacts to supplier operation and production due to extreme weather events
	Chronic		✓	✓	· Increased energy consumption due to rising average temperature · Damage to assets and impact on supplier operation and production arising from long-term changes in climate environment (e.g. precipitation patterns, temperature, or sea level)
Opportunity	Resource efficiency	✓	✓	✓	· Decreased operating costs due to use of operational models of higher efficiency
	Sources of energy	✓	✓	✓	· Reduced GHG emissions by adopting low-carbon energy sources
	Products/ services	✓	✓	✓	· Increased income thanks to development and/ or addition of low-carbon products and services (adoption of energy conservation measures in the supply chain included)
	Market	✓	✓	✓	· Motivated industrial transformation thanks to popularization of emerging technologies like 5G, IoT, and big data
	Resilience	✓	✓	✓	· Reduced impact from physical risks thanks to strengthened asset resilience

Note: The short-term is 2021-2025; the mid-term is 2026-2030; and the long-term is 2031-2050.

Material Climate Risks & Opportunities

RISKS

Policy and Legal Risks

Risk Impact Summary:

- According to the assessment results of climate change risks and opportunities, among the transition risks, policy and legal risk has the highest weight, making it the material risk. In addition, subject to the Climate Change Response Act, companies in Taiwan are to achieve net-zero emissions by 2050.
- In the IEA STEPs scenario, the estimated additional expenditures in 2025, 2030, 2040, and 2050 are NT$650 million, NT$3.945 billion, NT$8.393 billion, and NT$2.045 billion, respectively. In the IEA NZE scenario, the estimated additional expenditures in 2025, 2030, 2040, and 2050 are NT$1.447 billion, NT$7.891 billion, NT$6.398 billion, and NT$3.050 billion, respectively.

Risk Responses:

- The carbon reduction strategies are (1) improve energy efficiency and (2) use renewable energy. The carbon reduction plans include but are not limited to: improve the energy efficiency of IDC equipment, replace aged equipment and repair/optimize existing equipment and facilities, install and procure renewable energy project sites, procure pure renewable energy, renewable energy certificates, energy storage equipment development, and other projects and plans.
- According to the results of the carbon inventory, the Scope 1 and 2 GHG emissions in 2022 are 714,098 t-CO_2e, with a carbon reduction of 9.6% compared with the base year (2020). In the future, we shall continue to carry out comprehensive energy conservation and carbon reduction works on technology and personnel behavior to manage the possible impacts from such risk.

RISKS

Acute Risks

Risk Impact Summary:

- According to the assessment results of climate change risks and opportunities, among the physical risks, the acute risk has the highest weight, making it the material risk.
- According to IPCC's estimates and Taiwan's TCCIP information, landslides caused by precipitation at the intensity of typhoon may damage to assets of operating sites, IDCs, and base station assets of Chunghwa Telecom. Based on the assessment results, in the RCP 8.5 and RCP 2.6 climate scenarios, the potential financial impact of a strong typhoon on Chunghwa Telecom will amount to a minimum of NT$149 million per year.

Risk Responses:

- Formulate short-, medium-, and long-term climate change adaptation plans, and prepare budgets each year in line with the work progresses of the climate change adaptation plans.
- The climate change adaptation plans involve works either in the short, medium, or long term, including:

1. Flood/Disaster Prevention Action Plan for IDC Telecom Equipment and Building Facilities
2. Adaptation Action Plan for Line Facilities in Response to Climate Change
3. Adaptation Action plan for Telecom Base Station Networks in Response to Climate Change

OPPORTUNITIES

Sources of energy

Opportunity Impact Summary:

- According to the international organization, Statista, the income from the IDC market is projected to reach $342.1 billion in 2023, with the market scale to be $410.4 billion in 2027.
- In view of the fact that all countries and key international customers have set net-zero targets, in the IEA STEPs and IEA NZE climate scenarios, we can realize the growth of IDC business through the target of 100% IDCs on renewable energy by 2030.
- Assuming that the Compound Annual Growth Rate (CAGR) of revenue is 4.66%, in the duration of 2023 and 2027, we expect the revenue from IDCs will increase by NT$1.5 billion by 2027.
- After estimation of the demand for renewable energy from IDCs and calculation of the actual costs in renewable energy procurement, it is projected that the net profit will grow by approximately NT$1.2 billion by 2027.

Opportunity Responses:

- By improving energy efficiency and reducing power consumption from the source, projects include but are not limited to: improve the energy efficiency of IDC equipment, replace aged equipment and repair/optimize existing equipment and facilities, etc.
- Actively deploy renewable energy, including installation and procurement of renewable energy project sites, pure renewable energy procurement, renewable energy certificates, energy storage equipment development, and other projects to gradually elevate the percentage of renewable energy use.

Greenhouse Gas Emissions Management

Unit: t-CO_2e	2020	2021	2022
Direct emissions (Category 1)	22,192.93	17,887.47	**19,185.32**
Indirect emissions (Category 2)	768,128.07	716,979.26	**694,912.72**
Total emissions (Category 1+ Category 2)	790,321.00	734,866.73	**714,098.04**
Emission Intensity (t-CO_2e/NT$ in million)	3.8	3.5	**3.3**
Percentage of category in revenue	100%	100%	**100%**

Notes: 1. Indirect emissions (Category 2) are measured on a location-based method.
2. Category 1 emissions increased by about 7.26% in 2022 compared to 2021 levels mainly due to refrigerant replacement.
3. The decrease of total emission in 2022 shows that the switch from PSTN to SVG, the power consumption optimization which does not affect the network operation, the replacement of old access and high energy consumption base equipment, and reduction of IDC PUE.
4. The telecom industry we belong to has no emissions of ozone-depleting substances or other major gases.

Scope 3 Inventory and Verification

Emissions (t-CO_2e)

Upstream

Category 3

Upstream transportation and distribution
646.60

Downstream transportation and distribution
901.86

Business travel
1,174.65

Employee commuting
10,203.88

Category 4

Purchased goods and services
752,416.69

Capital goods
344,733.39

Fuel- and energy-related activities
124,456.91

Waste generated in operations
943.59

Upstream leased assets
13,045.93

Downstream

Category 5

Use of sold products
460,657.59

End-of-life treatment of sold products
1,403.50

Downstream leased assets
115,519.72

Investments
1,956.57

Total 1,828,060.88

Note: The Scope 3 inventory was expanded in 2022. The carbon emissions generated by products on consignment at the stores (including CPE, mobile phones, tablets, etc.) belonging to Scope 3 categories include (1.) purchased goods and services, (4.) upstream transportation and distribution, (9.) downstream transportation and distribution, (11.) use of sold products, and (12.) end-of-life treatment of sold products, totaled 305,676.97 metric tons.

Cybersecurity Risks

Driven by the Industry 4.0 development and emerging network applied technologies (e.g. 5G application, softwareization, virtualization/cloudification, and IoT), cybersecurity threats have evolved into multi-faceted mixed attacks that increase challenges for enterprises in cybersecurity management.

We continue to study and analyze measures for risk protection, align ourselves with international cybersecurity standards, and establish the joint defense mechanisms with governments and international cybersecurity organizations, effectively enhancing the overall cybersecurity defense and response capabilities of the Company. Furthermore, we are actively developing key information technology and strengthening supply chain security, which offer secured, reliable digital environment to our customers.

Corresponding Strategies

Aiming to achieve the cybersecurity vision of "establishing the most valuable, secure, reliable, and trustworthy telecom service provider that meets international standards," we implement "Cybersecurity Policy" and "Privacy Policy" right from the start. Pursuant to the spirit of ISO 27001 Information Security Management System, we achieve the goal of "zero tolerance" for both major cybersecurity breach and privacy incidents.

In addition, to ensure the security of "ICT systems" and "critical infrastructure," with reference to the NIST Cybersecurity Framework (CSF) and in pursuance of the standards and regulations, domestically and internationally, we established "Cybersecurity and Privacy Protection Risk Management Framework" to put in place specific and effective measures for cybersecurity and privacy protection so as to prevent any potential cybersecurity risk.

Our performance of cybersecurity and privacy risk management has been incorporated into the regularly tracking by the Risk Management Committee for management. Any material risk issue will be submitted to the Audit Committee or directly reported to the Board of Directors. There was no business impact or penalty arising from cybersecurity or privacy breach as of 2022. "Cybersecurity Insurance - Data Protection Insurance" has been purchased to protect the rights of customers and investors.

Opportunities and Actions

With the goal of "Attention & Implementation of Cybersecurity by All," we have incorporated "Information Security" in the KPIs for employees. Also, we regularly conduct internal/external audits and have passed inspections by competent authorities. At present, all of the IT infrastructures of Chunghwa Telecom are 100% certified to international cybersecurity standards (ISO 27001 / ISO 27011 / ISO 27017 / ISO 27018 / BS 10012 / CSA STAR Certifications).

For more information of the specific measures for cybersecurity and privacy protection, including Diversity and Defense-in-Depth for cybersecurity protection and management, intelligent security operation center, and cybersecurity threat detection and warning, critical infrastructure and ICT system Business continuity management, real-time incident report and rapid response mechanism, third-party vulnerability analysis and cybersecurity health diagnosis.

* For more information of cybersecurity and privacy policy, please refer to:

Cybersecurity Management Strategy and Structure

1 To ensure an effective operation of cybersecurity management, "Cybersecurity and Privacy Protection Management Committee" has been established at Chunghwa Telecom. A SEVP represents as the Chief Information Security Officer (CISO), dedicated to the supervision of matters concerning the Company's internal cybersecurity.

2 Meetings of "Cybersecurity Working Group" and "Privacy Protection Working Group" are held regularly to review appropriateness of the policy directions; oversee and assessment the compliance and effectiveness of management measures; and report to the Board of Directors.

4 Under the Cybersecurity and Privacy Protection Management Committee, the "Cybersecurity and Privacy Protection Executive Committee" and dedicated units are instituted in all Business Groups (Laboratories), supervised by the Deputy Cybersecurity Supervisors of Business Groups (Laboratories), to carry out and exercise various works for cybersecurity and privacy protection.

3 A department dedicated to ICT security management was approved to be set up to assess with the laws and regulations and technical development for new businesses, and coordinate matters concerning the companywide cybersecurity policies and regulations, risk control and management, cybersecurity surveillance and management, education and promotion, efficacy assessment, as well as compliance checks. The works of cybersecurity management are improved ceaselessly in line with the standards, laws, and regulations at home and abroad to reduce the corporate cybersecurity risks, offer a safe and reliable digital environment to customers.

Creation of the Most Valuable, Secure, and Reliable Digital Environment

- In the face of the increasing cybersecurity threat arising from geopolitics, Chunghwa Telecom actively responds to the government's policy of "information security is national security," allocating huge resources and cultivate cybersecurity talents and strengthening the cybersecurity resilience of critical infrastructure.
- Construct a smart cybersecurity monitoring platform, which successfully blocks approximately 20 million external attacks on a monthly basis, and work with C-ISAC, the national cybersecurity organization, for joint defense. In 2022, we shared 1,921 intelligences to lower the overall risk to hacking for the country and customers.
- Organize "Cybersecurity and Personal Data Protection" education and training and 2 email social engineering drills each year, along with requirement for all employees and contractors to 100% complete the training.
- Lay out the cybersecurity function map, design advanced training courses for different levels of managers and work areas, systematically strengthen employees' ICT security awareness, and comply with relevant regulations.
- In 2022, the advanced "Security Program Development Expert Cultivation Program" was initiated to incentivize employees to participate in the external security code competition and secure top three in the competition; the new, interactive application security training platform was also introduced to help developers think and write security codes with a security mindset in order to reduce security vulnerabilities, which is expected to train 200 experts in secure program development by 2023.