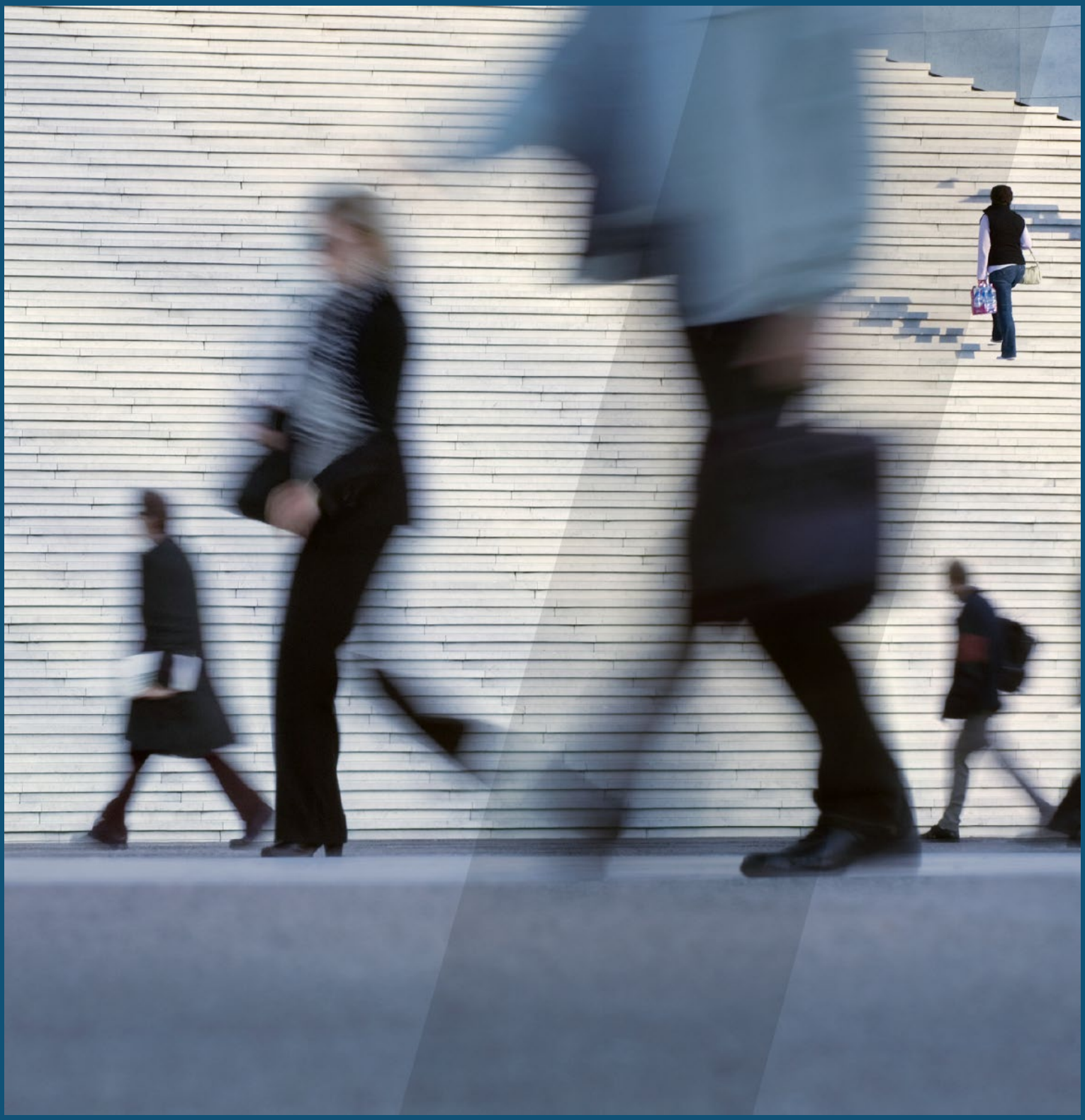


Technical Update in Taiwan

July 2026

forvis mazars
瑪澤聯合會計師事務所

Table of Content

Technical Update in Taiwan

1. Payroll

NEGOTIATED DEFERRAL OF RETIREMENT AGE OR POST-RETIREMENT REEMPLOYMENT

In response to Taiwan entering an aged society, policies are introduced to encourage older workers to remain in the workforce. The focus is on two employment models—"negotiated deferral of retirement age" or "post-retirement reemployment"—to provide both employers and employees with clear rights and a basis for negotiation.

Model 1: Negotiated Deferral of Retirement Age

This model applies when both employer and employee mutually agree to extend the mandatory retirement age stipulated in Article 54 of the Labor Standards Act before the employee reaches 65 years old.

Key Principles

- No Change to the Existing Employment Contract:

  Both parties continue to perform under the original open-ended (non-fixed-term) employment contract. The employee's years of service continue to accrue without interruption.

- Employment Conditions Cannot Be Unilaterally Changed:

  The employer may not unilaterally reduce wages, change job duties, or diminish existing benefits. If adjustments to job responsibilities require changes to employment conditions, such changes must be negotiated and agreed upon by both parties in good faith.

- Written Documentation Required:

  The agreed-upon postponed retirement age and related terms should be clearly documented in writing and retained to help prevent future labor-management disputes.

Model 2: Post-Retirement Reemployment

This model applies when an employee has already retired (settled prior seniority and received retirement benefits) and is later rehired by the same or a different employer.

Key Principles

- New Fixed-Term Employment Contract:

  Under the Middle-aged and Elderly Employment Promotion Act, an employer who rehires a retired worker aged 65 or older may enter into a fixed-term employment contract with the worker. The employee's length of service is recalculated from the date of reemployment.

- Protection of Basic Labor Rights:

  During the period of reemployment, wages, working hours, leave entitlements, and other employment conditions must continue to comply with the minimum standards prescribed by the Labor Standards Act.

- Mandatory Occupational Accident Insurance Coverage:

  In accordance with the Labor Occupational Accident Insurance and Protection Act, the employer must enroll the rehired older worker in occupational accident insurance on the employee's first day of work to ensure workplace safety and legal protection.

Technical Update in Taiwan
2. Corporate Secretarial Services

NEW LABOR TRAINING REQUIREMENT UNDER THE COMPANY ACT: KEY POINTS ON LABOR RIGHTS TRAINING

1. Legal Basis

To strengthen employers' awareness of labor laws and reduce labor disputes, Article 387-1 of the Company Act and Article 9-1 of the Business Registration Act were amended and promulgated on December 26, 2025, and will take effect on June 26, 2026.

2. Applicable Entities

- Companies and businesses established on or after June 26, 2026, are required to complete labor rights training.

- Companies and businesses established before June 26, 2026, are not subject to the mandatory requirement; however, participation is encouraged and a completion record may be reflected in the public registration records.

- The training requirement applies regardless of whether employees have been hired.

3. Training Requirements

- No statutory deadline or penalty is currently prescribed; however, companies and businesses are encouraged to complete the training as soon as practicable.

- Completion of at least one approved course is required. Both online and in-person courses are accepted, and there is no minimum course duration requirement.

- Course fees, if any, are determined by the respective training providers.

4. Recognized Courses

Currently, all courses available through the "e-Learning Platform for Labor Education" and designated courses under the "Labor Rights Training" program offered by the SME Learning are recognized by the Small

and Medium Enterprise and Startup Administration. Additional recognized courses may be announced by the authority from time to time.

5. Participants and Record Annotation

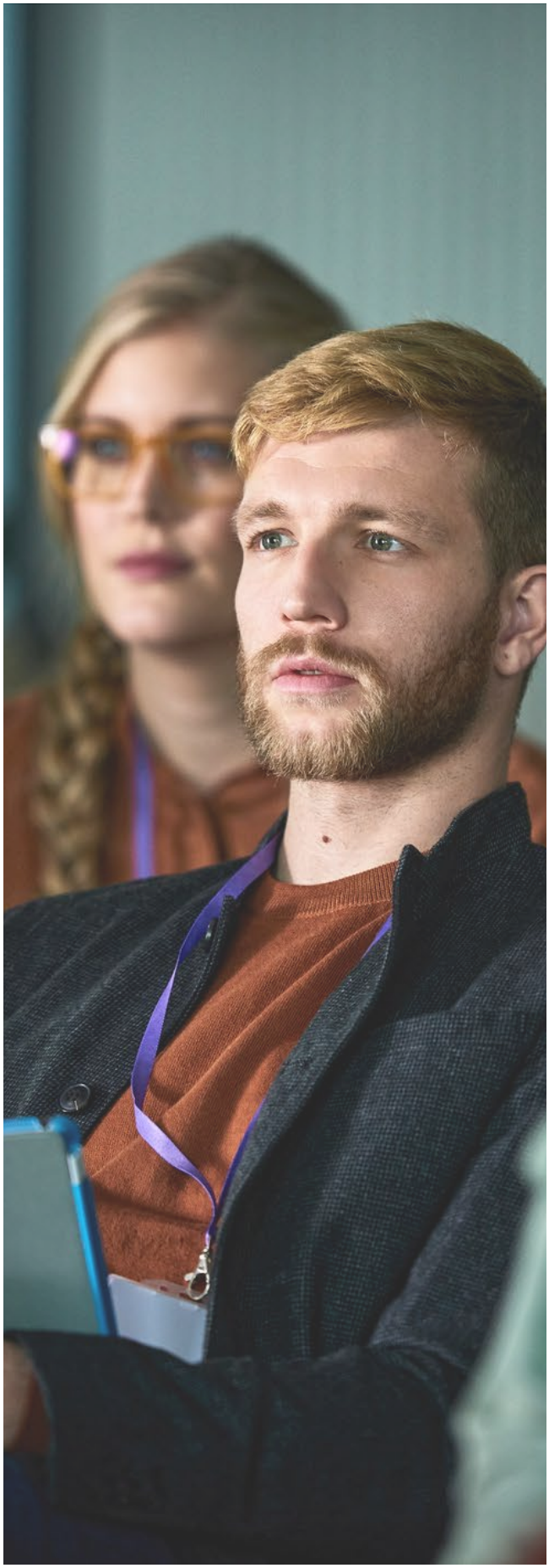
The law does not specify who must attend the training. However, it is recommended that the responsible person of the company/business or human resources personnel participate in the course.

Upon completion of the training, the training provider will submit the relevant information to the competent authority, and the Administration of Commerce, MOEA will automatically update the completion record on the Ministry of Economic Affairs' Get information about business Registration in Taiwan.

6. Other Important Notes

Only one training course is required, and there is no requirement for periodic retraining or renewal of the completion record.

For courses completed between December 26, 2025 and June 26, 2026, participants may request the training provider to submit the relevant information for record annotation. Courses completed before December 26, 2025 are not eligible for retrospective annotation.



Technical Update in Taiwan

3. Audit

FROM CYBERSECURITY INCIDENT TO AUDIT RESPONSE: FINANCIAL REPORTING AND AUDIT IMPLICATIONS OF RANSOMWARE ATTACKS

1. Introduction

In recent years, organizations worldwide have faced an increasing number of cybersecurity threats, with ransomware attacks emerging as one of the most prevalent and disruptive forms of cyber incidents. Taiwan has not been immune to this trend. Numerous listed companies have publicly disclosed ransomware attacks, data breaches, and information system disruptions, some of which have resulted in operational interruptions, production shutdowns, or complete system outages.

In communicating such incidents to investors and stakeholders, affected companies often emphasize that the impact on operations and financial performance is limited. However, from a financial reporting and financial statement audit perspective, the risks arising from cybersecurity incidents frequently extend beyond information technology concerns. Such incidents may affect the integrity of accounting records, the effectiveness of internal controls, the reliability of financial information, and management's significant estimates and judgments.

Accordingly, when a significant cybersecurity incident occurs at an audit client, auditors should consider it a risk factor that may affect the financial statements and should reassess risk assessments and design appropriate audit responses as necessary.

2. Cybersecurity Incidents Are Audit Issues, Not Merely Information Security Issues

Under ISA 315, Identifying and Assessing the Risks of Material Misstatement, auditors are required to obtain an understanding of the entity's information system and related controls in order to identify risks that may result in material misstatements in the financial statements.

When an organization experiences a ransomware attack, the financial reporting process may be exposed to the following risks:

(1) Impairment of Accounting Data Integrity

Ransomware attacks typically encrypt corporate databases and servers. If affected systems include the ERP system, general ledger, or related sub-ledgers, the following consequences may arise:

- Loss of transaction data
- Inaccessibility of financial records
- Incomplete backup data
- Disruption of audit trails

Under these circumstances, auditors should reassess the reliability of accounting records and evaluate whether management-provided financial information remains suitable as a source of audit evidence.

(2) Unauthorized Modification of Financial Information

If attackers obtain administrative privileges, they may be able to alter:

- Vendor master data
- Payment instructions and banking information
- Inventory records
- User access rights and permissions

Such circumstances not only increase the risk of error but may also elevate fraud risk, thereby affecting the auditor's overall risk assessment.

(3) Breakdown of Internal Controls

Following a cyber incident, organizations often implement emergency response measures, such as:

- Granting emergency administrator access
- Disabling certain system controls
- Processing transactions manually
- Establishing temporary operating procedures

As a result, controls previously tested and determined to be effective may no longer operate effectively on an ongoing basis.

3. Potential Financial Reporting Implications of Ransomware Attacks

The financial reporting implications of cybersecurity incidents often extend beyond direct ransom payments and may involve a variety of accounting considerations.

(1) Recognition of Operating Expenses and Losses

During the incident response and recovery process, organizations may incur:

- Cybersecurity consulting fees
- System restoration and recovery costs
- Legal advisory fees
- Public relations and crisis management expenses

Auditors should evaluate whether the accounting treatment of these expenditures is appropriate.

(2) Assessment of Liabilities and Contingencies

Where the incident involves:

- Personal data breaches
- Customer claims or litigation
- Regulatory investigations and penalties

Management may need to assess whether a liability should be recognized or a contingent liability disclosed in accordance

with IAS 37, *Provisions, Contingent Liabilities and Contingent Assets.*

(3) Asset Impairment Assessment

Where a cybersecurity incident results in:

- Prolonged operational disruption
- Loss of significant customers
- Reduced expected future cash flows

the recoverable amount of goodwill, intangible assets, or other long-lived assets may be affected.

(4) Going Concern Considerations

Although many organizations recover from cybersecurity incidents within a relatively short period, severe attacks may result in prolonged business interruption, significant revenue losses, or financing difficulties. In such circumstances, the entity's ability to continue as a going concern may be called into question.

4. Auditor Responses to a Significant Cybersecurity Incident

When a significant cybersecurity incident occurs, auditors should consider whether revisions to the audit strategy and additional audit procedures are necessary.

(1) Understanding the Nature and Extent of the Incident

The audit team should obtain a thorough understanding of the incident, including:

- The timing of the incident
- The nature of the attack
- The systems affected
- The progress of recovery efforts
- Whether financial reporting systems were impacted

In addition to management's explanations, auditors should review supporting documentation such as:

- Incident Response Reports
- Digital Forensic Investigation Reports
- Audit Committee and Board of Directors meeting minutes

to obtain more objective and corroborative information.

(2) Reassessing the Reliability of Audit Evidence

Where accounting systems have been compromised or encrypted, auditors should consider:

- Whether transaction data remains complete
- Whether backup data is available and reliable
- Whether system restoration procedures were appropriately performed
- Whether information obtained during the audit remains reliable

Additional substantive procedures may be required to reduce audit risk to an acceptable level.

(3) Reassessing Reliance on Internal Controls

If the incident results in:

- Failure of key controls
- Suspension of automated controls
- Significant manual intervention in transaction processing

auditors may need to reduce reliance on internal controls and expand substantive testing procedures.

5. Subsequent Events Considerations

Some cybersecurity incidents may only be identified after the reporting date.
For example:

- Financial statement date: December 31, 2026
- Ransomware attack discovered: January 15, 2027

In such circumstances, auditors should evaluate the incident under ISA 560, Subsequent Events, including whether:

- The incident provides evidence of conditions that existed at the reporting date
- Adjustments to the financial statements are required
- Additional disclosures are necessary

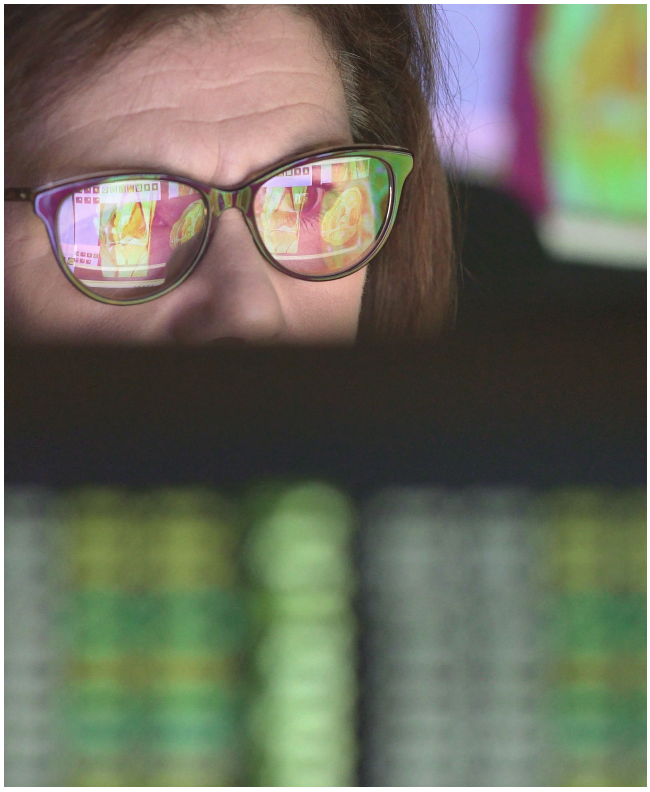
Particular attention should be given to situations where subsequent investigations indicate that attackers had gained access to the company's systems prior to the reporting date.

6. Conclusion

As organizations become increasingly dependent on digital technologies, cyberattacks have emerged as a significant business risk that can no longer be ignored. For auditors, significant cybersecurity incidents should not be viewed solely as information technology issues. Rather, auditors should evaluate their potential effects on financial reporting and the financial statement audit.

When a client experiences a ransomware attack, auditors should reconsider their assessment of the risks of material misstatement and evaluate the impact on the reliability of accounting records, the effectiveness of internal controls, and subsequent event considerations. Based on this assessment, auditors should determine whether modifications to the planned audit approach are necessary.

Ultimately, the key question facing auditors is no longer whether organizations will experience cyberattacks, but whether audit teams are adequately prepared to evaluate the implications of such incidents for financial reporting and audit execution.



4. Tax

INHERITED OR GIFTED PROPERTIES UNDER THE OLD TAX REGIME MAY NOW APPLY CPI-ADJUSTED COST BASIS UPON DISPOSAL

Summary

On July 15, 2026, the Ministry of Finance issued tax ruling (Tai-Cai-Shui-Zi No. 11504549440) providing that where an individual sells a house acquired by inheritance or gift, and the actual transaction price at the time of sale has been provided by the taxpayer or ascertained by the tax authority, and the house transaction income is taxed under the old regime, the taxable income may be computed by analogy to the new House and Land Transactions Income Tax regime.

That is, the income shall be the sale price of the house, less the assessed current value of the house at the time of inheritance or gift as adjusted by the Consumer Price Index (CPI), and less the expenses incurred for the acquisition, improvement, and transfer of the house.

Analysis

Under Taiwan's current consolidated housing and land income tax regime (the "new regime"), individuals selling inherited or gifted real estate are allowed to adjust both the property's assessed value and the government's announced land value at the time of inheritance or gift based on changes in the Consumer Price Index when calculating taxable gains.

To align the treatment of properties subject to the old tax regime with the principles of the new regime, the MOF's latest ruling extends a similar CPI adjustment mechanism to inherited or gifted properties taxed under the old rules. Where the actual selling price of the property has been substantiated or verified by the tax authority, the property's assessed value at the time of inheritance or gift may be adjusted according to the ratio between the CPI in the month of sale and the CPI in the month of inheritance or gift. The adjusted amount may then be deducted from the selling price when determining taxable income, thereby mitigating the impact of inflation on taxable gains.

Illustrative Example

Mr. John Doe inherited a house in May 2014 (assessed current value of the house at the time of inheritance: NT$950,000; CPI: 95). He sold the house in March 2026 for NT$4,000,000 (necessary expenses at the time of sale: NT$0; CPI: 110). The house transaction income is computed as follows:

	Sale Price (A)	Assessed Current Value at Inheritance (B)	CPI Adjustment (C)	Transaction Income (D) = (A) – (B*C)
Before the ruling	NT$4,000,000	NT$950,000	–	NT$3,050,000
After the ruling	NT$4,000,000	NT$950,000	110 / 95	NT$2,900,000

*Calculated as NT$4,000,000 – (NT$950,000 × 110/95) = NT$2,900,000.

Our Observations

This new ruling further harmonises the treatment of property transaction costs under the old property transaction tax regime with that of the current consolidated housing and land income tax system. By allowing the assessed property value at the time of inheritance or gift to be adjusted for inflation, the ruling helps reduce the taxation of purely nominal gains resulting from long-term price increases.

Individuals planning to dispose of inherited or gifted properties should carefully review the applicable cost calculation method, as the new approach may significantly reduce their taxable gains and overall tax burden.

Disclaimer

The information contained, and views expressed, herein are for general guidance only, and are not to be construed as representing a professional opinion of Forvis Mazars. No responsibility is accepted for any errors or omissions, howsoever caused, that this publication may contain, or for any losses sustained by any person as a result of reliance on any information contained herein.

Contacts

Al Chang
Managing Partner, Head of Tax
Al.chang@forvismazars.com

Andrew Chu
Partner, Assurance & Audit Services
Andrew.chu@forvismazars.com

Lisa Liu
Partner, Accounting & Outsourcing Services
Lisa.liu@forvismazars.com

Eric Chou
Partner, Assurance & Audit Services
Eric.chou@forvismazars.com

Forvis Mazars is a leading global professional services network operating under a single brand with just two members: Forvis Mazars, LLP in the United States of America and Forvis Mazars Group SC, an internationally integrated partnership operating in over 100 countries and territories. Both members share a commitment to providing an unmatched client experience, delivering audit & assurance, tax, advisory and consulting services across the globe.
Visit forvismazars.com to learn more.

forvis mazars
瑪澤聯合會計師事務所