TECHMAIL

2025 1st Issue

Official publication of the Chartered Governance and Accountancy Institute in Zimbabwe

Issuance of Clearance Certificates for Professionals

The Zimbabwe Revenue Authority (ZIMRA) hereby advises all employers, professionals and professional bodies that in line with Public Notice Number 92 of 2024, the guidelines for issuance of clearances have been uploaded on the ZIMRA website. ZIMRA's computerised systems are not fully equipped to process this requirement for 2025 and interim guidelines have been established to facilitate manual clearances until further notice.

Criteria for Issuing Clearance Certificates

Clearance Certificates will be issued under the following conditions:

1. The applicant is fully tax compliant, i.e. including registration, submission of returns, and payment of tax.

2. Employees of organizations who do not earn additional taxable income from other sources.

3. Employees earning income from other sources, provided they are tax compliant.

Interim Guidelines

1. Professionals in Trade

a) Professionals conducting business are required to register for tax and apply for a Tax Clearance Certificate via TaRMS.

b) Professionals with a Tax Clearance Certificate older than 30 days must submit a manual application and will be issued a confirmation letter for registration and licensing purposes.

2. Employees

a) Employees who are professionals must complete a manual application form.

b) Employers with multiple professionals needing clearance letters must submit a list of all employees applying for clearances, accompanied by a covering letter and individual application forms. Upon approval, ZIMRA will issue a letter to the employer, which will serve as a Clearance Certificate for licensing purposes.

3. ZIMRA Processing

a. Dedicated units at local ZIMRA stations will handle the processing of these applications.

b. Applications should be submitted via email to contactcentre@zimra.co.zw for processing.

Key Information:

- The confirmation letter issued by ZIMRA will act as a valid Clearance Certificate for the purpose of registration and licensing with professional bodies only.
- Compliance with this requirement is compulsory for professional registration and licensing.

For any inquiries or further clarification, taxpayers are encouraged to contact their nearest ZIMRA Offices or get in touch with the ZIMRA Contact Centre on the details provided below.

Membership Re-Application	US$100
Election fee	US$120
Graduates (Grad.CG)	US$180
Associates (ACG)	US$245
Fellow (FCG)	US$260

Renew or upgrade your membership and be included in the Institute directory. To check your membership status in the directory, visit (https://mycgizim.org/verifications). If you have any other inquiries about your membership status or need an invoice, please send an email to nmazaiwana@cgizim.org or tmushonga@cgizim.org.

+263 242 700 553-5
+263 716 317 675

cgizim@cgizim.org
www.cgizim.org

Harare: 22 - 32 McChlery Avenue, Eastlea
Bulawayo: 73 A Ailsa Court, J Tongogara St/ L Takawira Ave,

Understanding the New Cyber Crimes Bill in Zimbabwe

Introduction

The Cyber Crimes Bill, recently passed into law in Zimbabwe, aims to combat cybercrime and enhance online security. As professionals in the field, it's essential to understand the implications of this law on our daily activities and businesses.

Key Provisions

- **Cybercrime Offences**

  The Bill outlines various cybercrime offences, including unauthorized access to computer systems, data interference, and cyber harassment.

- **Investigation and Prosecution**

  Law enforcement agencies will have enhanced powers to investigate and prosecute cybercrime cases.

- **Penalties.**

  Severe penalties, including fines and imprisonment, will be imposed on those found guilty of cybercrime offences.

- **Reporting Obligations**

  Certain entities, such as financial institutions and critical infrastructure providers, will be required to report cybercrime incidents.

Guidance for Members and Stakeholdes

- **Implement Robust Cybersecurity Measures**

  Ensure your organization has adequate cybersecurity measures in place to prevent and detect cybercrime.

- **Train Employees**

  Educate employees on cybercrime risks and best practices.

- **Report Incidents**

  Familiarize yourself with reporting obligations and procedures.

- **Stay Informed**

  Regularly update yourself on the latest cybercrime trends and threats.

Recommendations

- Consult with cybersecurity experts to ensure compliance with the new law.
- Develop incident response plans.
- Stay vigilant and report suspicious activities.

Developing incident response plans

Steps to Develop Incident Response Plans

i) Identify Potential Incidents

Determine types of incidents that could occur (e.g., data breaches, ransomware attacks).

ii) Establish a Response Team

Assemble a team with defined roles and responsibilities.

iii) Define Incident Response Procedures

Outline steps to take during an incident (e.g., containment, eradication, recovery).

iv) Develop Communication Plan

Establish communication protocols for stakeholders, including employees, customers, and law enforcement.

v) Test and Update Plan

Regularly test and update the plan to ensure effectiveness.

Example 1: Data Breach Incident Response Plan

a) **Detection:** Identify potential data breach through monitoring or reporting.

b) **Containment:** Isolate affected systems or data.

c) **Assessment:** Determine scope of breach and affected data.

d) **Notification:** Inform stakeholders, including customers and regulatory bodies.

e) **Eradication:** Remove root cause of breach.

f) **Recovery:** Restore systems and data.

Example 2: Ransomware Attack Incident Response Plan

a) **Detection:** Identify ransomware attack through monitoring or reporting.

b) **Containment:** Isolate affected systems.

c) **Assessment:** Determine scope of attack and affected data.

d) **Notification:** Inform stakeholders, including employees and management.

e) **Eradication:** Remove malware and restore systems.

f) **Recovery:** Restore data from backups.

Key Components

1. Clear Roles and Responsibilities: Define team members' roles.
2. Communication Plan: Establish communication protocols.
3. Incident Classification: Categorize incidents based on severity.
4. Training and Testing: Regularly train and test the response team.

By following these steps and examples, you can develop effective incident response plans to minimize the impact of security incidents.

Conclusion

The Cyber Crimes Bill is a significant step towards combating cybercrime in Zimbabwe. By understanding the provisions and taking proactive measures, we can enhance online security and protect our organizations and individuals from cyber threats.

By working together, we can create a safer online environment in Zimbabwe.

Bindura University of Science Education

Chartered Governance and Accountancy Institute in Zimbabwe

CALL FOR PAPERS

Theme

"Revitalising Industries: Driving Innovation for a Sustainable Future"

23 - 25 July 2025

Montclair Hotel and Casino, Nyanga, Zimbabwe

About the Conference

The International Business, Governance & Accounting Conference is an annual multidisciplinary international event that serves as a nexus for expertise, bringing together thought leaders, academics, innovators, business practitioners, post graduate students and non-governmental organisations representatives. It's an avenue where experts present new research, innovative tools, and evolving industry norms. The outcomes of the conference will contribute to revitalizing industries in Zimbabwe and the region at large.

For more information

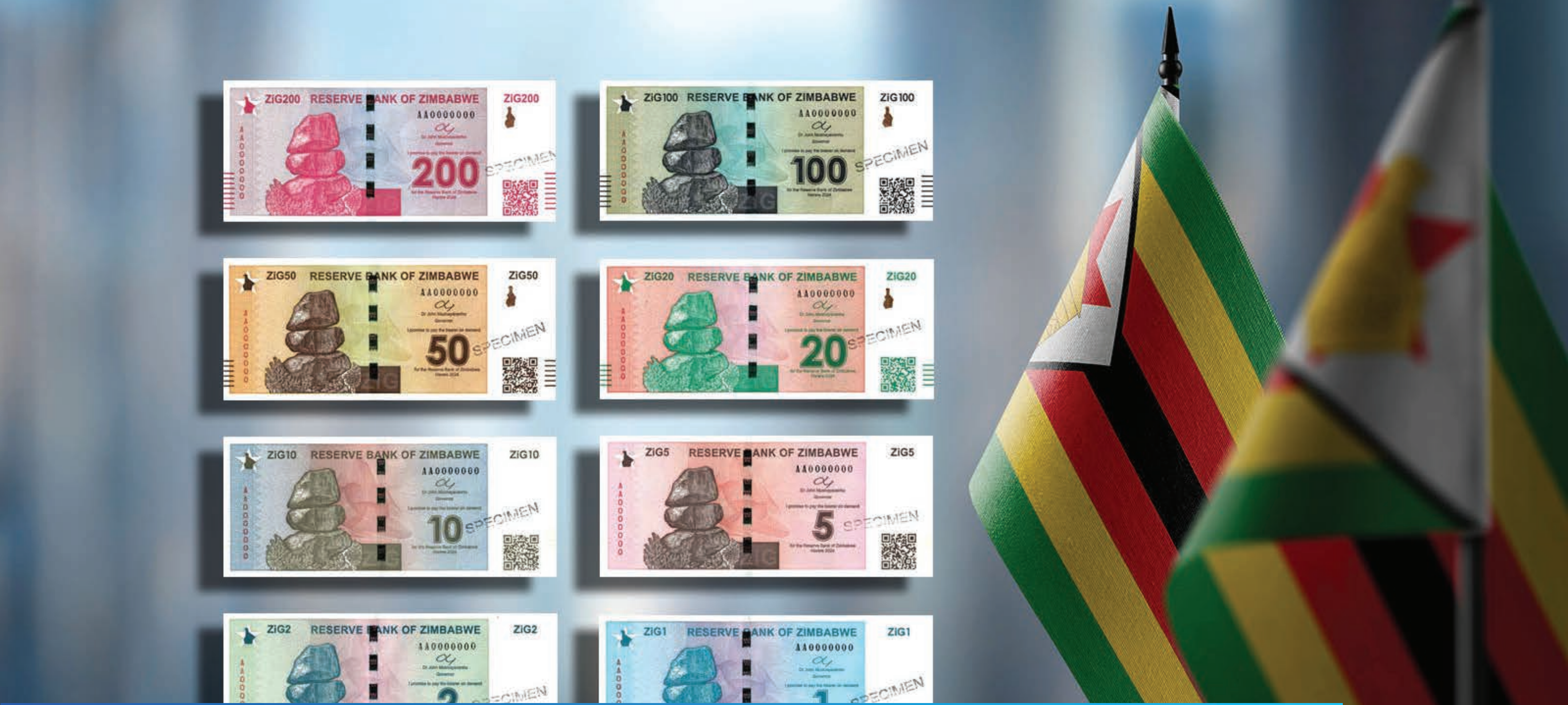
Ms. Metricia S. Rerayi +263785906098
Email: *mrerayi@cgizim.org*
Ms. Tendai Towo +263772734713
Email: *ttowo@buse.ac.zw*

Who Should Attend?

1. Innovation & Technology: Leveraging tech, AI, and automation for industrial growth.
2. Sustainability: Focusing on green practices, renewable energy, circular economies, and ethical innovation.
3. Policy & Financing: Reforming regulations and exploring funding models to boost business competitiveness.
4. Human Capital & Collaboration: Empowering workforce skills and fostering public-private partnerships for sustainable growth.
5. Digital Transformation: Driving progress through smart industry and digital tools.
6. Social Responsibility: Promoting ethical practices and cross-sector collaboration.

The scope of research may be theoretical or applied research and the research papers may range from original research papers, survey papers, case studies and academic or scholarly articles, to extended versions of previously published papers in conferences. Submit abstracts (200-300 words) to ibgac@buse.ac.zw , cc ttowo@buse.ac.zw and mrerayi@cgizim.org by 30th April, with full papers due by 13th June and conference fees payable by 11th July.

Visit our website for more information
www.buse.ac.zw or www.cgizim.org



Shaping the Future of the Profession: Critical Technical Trends for CGI Zimbabwe Students and Members

As the governance, accounting, and compliance landscape evolves globally, CGI Zimbabwe students and members must continuously align their skills, knowledge, and outlook with the emerging demands of modern professional practice. Today's challenges—from sustainability reporting to digital disruption—require more than just technical expertise. They call for adaptability, foresight, and an unrelenting commitment to lifelong learning.

Whether in public or private service, professionals are now expected to demonstrate interdisciplinary competence, digital agility, and strategic insight. Below are key technical themes that should be high on the radar of every governance and accountancy professional—and which form a compelling case for structured Continuous Professional Development (CPD).

1. Sustainability and ESG Reporting: A New Financial Language

The push for sustainable development and climate action is reshaping how performance is measured and reported. Professionals must be equipped to:

- Interpret and apply global sustainability reporting frameworks such as GRI, ISSB Standards, TCFD, and Integrated Reporting.

- Guide entities in identifying material ESG issues and embedding them into governance, risk, and compliance structures.

- Support public and private institutions in aligning their sustainability disclosures with national development strategies and SDGs.

2. Public Financial Management Reform and IPSAS Implementation

Zimbabwe's ongoing transition to accrual-based IPSAS by 2025 represents a significant milestone in public sector governance. This reform demands:

- Technical mastery of IPSAS principles and their application in budgeting, reporting, and auditing.

- Familiarity with the Public Finance Management Act, Treasury Circulars, and the constitutional provisions underpinning fiscal accountability.

- Professional development through programs like the Public Sector Accounting (PSA) Program to meet institutional capacity needs.

3. Technology, Data & AI: The Digital Professional's Toolkit

The rise of automation, AI, and data analytics is transforming traditional finance and governance roles. To stay relevant, professionals must:

- Develop competence in data management, analytics tools, and process automation.

- Understand the digital risks including cybersecurity, data privacy, and regulatory tech.

- Embrace digital transformation initiatives within their institutions and encourage digital ethics.

4. Governance, Risk & Compliance (GRC): Strategic and Operational Integration

Effective governance requires aligning risk, compliance, and ethics into the daily operations of institutions. Key focus areas include:

- Building robust internal control systems and governance structures.

- Managing compliance in procurement, anti-money laundering (AML), tax, and financial reporting.

- Identifying and mitigating emerging risks including ESG, political, and technological risks.

CPD Focus Area: GRC Frameworks, Internal Controls, Ethics and Regulatory Compliance.

5. Ethical Leadership and Professional Judgment

Ethics remains a cornerstone of professional identity. In a world increasingly exposed to fraud, corruption, and greenwashing, professionals must:

- Apply codes of ethics consistently across professional scenarios.

- Serve as ethical stewards in both public and private sector environments.

- Promote accountability, transparency, and public trust through informed, values-based decisions.

Final Word: Preparing for the Future of Work

The profession is shifting toward roles that demand agility, innovation, and purpose. Students and members of CGI Zimbabwe must embrace:

- Lifelong learning through structured CPD.

- Professional agility to navigate career transitions in a digital, climate-conscious economy.

- Values-based leadership as a hallmark of true professional influence.

CGI Zimbabwe continues to support this transformation through:

- Dynamic qualifications including CGPA, PSA, DFA, and GRC programs.

- Regional and global partnerships focused on sustainability, ethics, and innovation.

- Continuous knowledge-sharing through bulletins, webinars, and practical training.

Let us all rise to the challenge and shape a profession that is not only future-proof but future-driven.

By Richard Ndebele
Manager: Technical, Research, and Quality Assurance
CGI Zimbabwe

A proven facilitator with experience in training over 50,000 beneficiaries in financial literacy, savings, and business development. A dedicated and detail-oriented researcher, tech-savvy professional, and efficient worker with a passion for innovation and a strong commitment to sustainability reporting and artificial intelligence.

CONTACT US

Tel: 242 700 553-5 (Harare)
292 261 390 (Bulawayo)
WhatsApp : +263 71 631 7675

Email : cgizim@cgizim.org
ejonga@cgizim.org
rndebele@cgizim.org
dkandemwa@cgizim.org
Website : www.cgizim.org

CGI Head Office : Dzidzo House
22 - 32 Mchlery Avenues, Eastlea,
Harare.
CGI Bulawayo : 73A Ailsa Court,
J Tongogara St/L Takawira Ave
Bulawayo.