BELGIUM CAMPUS iTversity

Postgraduate Diploma in Cybersecurity Risk Management

NQF Level 8 | 120 Credits | Postgraduate Diploma

Value proposition: Strategic. Applied. Risk-focused.

The Postgraduate Diploma in Cybersecurity Risk Management develops advanced capability in cybersecurity risk management, governance and compliance, aligned with current frameworks and regulatory environments. Through applied research and the development of both technical and organisational decision-making skills, the programme prepares graduates for strategic roles and progression into Master's level study.

Qualification Overview

The Postgraduate Diploma in Cybersecurity Risk Management develops advanced capability to identify, analyse and manage cybersecurity risks at organisational and strategic levels. Designed for graduates and professionals who want to move beyond technical cybersecurity, the programme builds competence in governance, risk, compliance and information assurance, enabling students to align cybersecurity practices with organisational objectives.

Delivered fully online through scheduled live sessions, the programme offers consistent academic quality, practical learning, and direct access to expert lecturers to prepare you for workplace contribution and further study.

Delivered fully online through scheduled, live late afternoon and early evening sessions, it offers structured, real-time engagement with expert lecturers and provides a high-quality, flexible learning experience suited to working professionals.

Programme Structure and Components

The qualification comprises 120 credits, structured to develop advanced knowledge and applied capability in cybersecurity risk management, governance, and organisational security.

The programme is organised into a set of core modules, supported by an applied research project, ensuring both conceptual depth and practical application.

BELGIUM CAMPUS iTversity

Core Modules (90 Credits)

All modules are compulsory and focus on developing integrated capability across cybersecurity governance, risk management and organisational security contexts.

- **Principles of Research 582 (PRP582)** -15 Credits.
- **Introduction to Cyber Security 582 (ICB582)** - 15 Credits.
- **Cybersecurity Governance Frameworks 582 (CGF582)** - 15 Credits (Prerequisite: ICB582).
- **Information Assurance and Risk Management 582 (IAR582)** - 15 Credits.
- **Cybersecurity Laws and Regulatory Compliance 582 (CLR582)** - 15 Credits.
- **Ethics in Cybersecurity Risk Management 582 (ECB582)** - 15 Credits.

Applied Research Project (30 Credits)

The project serves as a bridge between academic learning and organisational application.

- **Cybersecurity Risk Management Research Project 582 (CRR582) -** 30 Credits.

Applied and Research Integration

The programme integrates conceptual understanding with applied capability across all modules, with a strong focus on organisational cybersecurity risk management. The Cybersecurity Risk Management Research Project is a central component of the qualification and enables students to investigate and address a cybersecurity risk-related challenge within an organisational or industry context.

Through this integrated approach, students develop:

- Advanced analytical and critical thinking capability.
- The ability to assess and manage cybersecurity risks with in organisations.
- Practical problem-solving skills aligned to governance and compliance environments.
- The ability to translate theory into structured, value-adding solutions.

Where appropriate, projects may be aligned to workplace or industry contexts, ensuring that learning is directly applicable and outcome driven.

Key Features

The programme is structured to deliver depth, relevance and organisational impact through the following key features:

- A strong focus on cybersecurity risk management, governance and compliance.
- Alignment with current cybersecurity frameworks, standards and regulatory environments.
- Development of both technical understanding and organisational decision-making capability.
- Applied research component focused on real-world cybersecurity challenges.
- Preparation for strategic and advisory roles in cybersecurity.
- Clear progression pathway into Master's-level study.

BELGIUM CAMPUS iTversity

Integrated Approach to Applied Learning and Industry Engagement

The programme maintains strong alignment with industry practice, governance requirements and organisational cybersecurity needs by integrating applied learning, engagement with the cyber security laboratory and structured industry interaction. Students work with current frame works, standards and regulatory environments, develop governance and risk focused decision making capability, and apply their learning through real-world scenarios and the Cybersecurity Risk Management Research Project, ensuring they can translate cybersecurity risk frameworks into practical organisational solutions.

Key elements include:

- Engagement with a dedicated cybersecurity laboratory environment to support applied learning.
- Alignment with current cybersecurity frameworks, standards and regulatory environments.
- A strong focus on governance, risk management and organisational decision-making.
- Development of applied and strategic capability within real-world contexts.
- Case based learning grounded in organisational scenarios.
- Exposure to current cybersecurity tools, standards and risk practices.
- Participation in masterclasses, guest sessions and roundtable discussions with industry practitioners.
- Applied research addressing organisational risk scenarios, governance challenges or compliance requirements.
- Analysis, simulation and evaluation supported by the cybersecurity laboratory environment.

Cybersecurity Laboratory Environment

Students benefit from a dedicated cybersecurity laboratory environment that provides practical, hands-on learning through real-world threat simulation, experimentation and applied skills development, ensuring strong alignment with industry expectations and preparing graduates for immediate contribution in professional environments.

The lab enables:

- Simulation of real-world cyber threats and attack scenarios.
- Practical testing of security tools, frameworks and techniques.
- Safe environments for experimentation, analysis and response.
- Development of applied skills in both network and software security contexts.

What Makes This Programme Different

The programme is designed to develop strategic cybersecurity capability through:

- **Risk-focused approach.** Strong emphasis on governance, compliance and organisational risk management.
- **Applied research component.** Focus on solving real cybersecurity challenges.
- **Integrated capability development.** Alignment of technical, legal, ethical, and organisational perspectives.

BELGIUM CAMPUS iTversity

- **Industry-aligned design.** Reflects current cybersecurity demands and regulatory environments.
- **Specialised institutional context.** Delivered within a focused ICT institution with strong industry engagement
- **Progression to Master's study.** Provides a foundation for research-based postgraduate qualifications

What You Will Develop

Through this programme, graduates will develop the knowledge, skills and professional capability required to operate effectively within cybersecurity environments and contribute to organisational resilience. Graduates will develop:

- The ability to analyse and manage cybersecurity risks within organisations.
- Advanced analytical and decision-making capability
- Knowledge of cybersecurity governance frameworks and compliance requirements.
- The ability to align cybersecurity strategies with business objectives.
- Strong communication skills across technical and non-technical stakeholders.
- Ethical and professional judgement in cybersecurity practice.

Who Should Apply and Career Outcomes

This qualification is suited to individuals who have completed prior studies in information technology or a related field and wish to specialise in cybersecurity risk management, governance, and organisational security

It is particularly relevant for:

- IT professionals seeking to specialise in cybersecurity risk management and governance.
- Professionals transitioning into cybersecurity roles with a focus on organisational impact.
- Individuals aiming to move into governance, risk and compliance (GRC) functions.
- Mid-career professionals seeking to strengthen their strategic and analytical capability in cybersecurity.

On completion, graduates are equipped to contribute at both operational and strategic levels within cybersecurity environments and may pursue roles such as:

- **Cybersecurity Analyst.**
- **Information Security Officer.**
- **IT Risk Manager.**
- **Cybersecurity Governance Specialist.**
- **Compliance and Regulatory Analyst.**
- **Cybersecurity Consultant.**

Graduates are able to support organisational resilience by identifying, analysing and managing cybersecurity risks, while aligning security practices with governance frameworks and business objectives.

Further Study Opportunities

On completion of this qualification, graduates may progress to a Master of Information Technology (NQF Level 9) or related research-based qualifications, subject to meeting admission and research readiness requirements.

This qualification forms part of a structured postgraduate pathway at Belgium Campus iTversity, enabling continued development from applied and strategic capability toward advanced research and innovation.

Why Study This Qualification

This programme is designed to develop advanced, in-demand capability in cybersecurity risk management, supporting both immediate impact in the workplace and progression into senior and specialised roles.

Key reasons to consider this qualification include:

- Develop specialised expertise in a high-demand and rapidly evolving field.
- Build capability in cybersecurity governance, risk management, and regulatory compliance.
- Strengthen analytical, strategic, and decision-making skills with in organisational contexts.
- Apply cybersecurity frameworks to real-world business and risk challenges.
- Prepare for roles that support organisational resilience and digital risk management.
- Establish a strong foundation for progression into Master's-level study and advanced specialisation.

Admission Requirements

To be considered for admission into the Postgraduate Diploma in Cybersecurity Risk Management, applicants must have successfully completed:

- A 360-credit or 480-credit Bachelor's Degree in Information Technology or a related field; or
- An Advanced Diploma (NQF Level 7) in Information Technology or a related field, including the Advanced Diploma in Cybersecurity

A minimum overall average of 60% is required for admission.

Applicants should demonstrate a strong foundation in areas such as:

- **Computer Networking.**
- **Information Technology.**
- **Information and Communications Technology.**
- **Network Management.**
- **Cybersecurity or related ICT disciplines.**

Admission is subject to alignment between the applicant's prior learning and the technical requirements of the programme.

Recognition of Prior Learning (RPL)

Belgium Campus iTversity recognises that applicants may have acquired relevant knowledge and skills through formal, informal, or work-based learning. In line with the policy framework of the South African Qualifications Authority (SAQA) and quality assurance requirements of the Council on Higher Education (CHE), Recognition of Prior Learning (RPL) may be applied in the following ways:

BELGIUM CAMPUS iTversity

RPL for Access (Admission Equivalence)

Applicants who do not meet the formal NQF Level 7 entry requirements may be considered for admission based on demonstrated equivalence. This process evaluates whether the applicant's prior earning, professional experience and competencies are comparable to the expected outcomes of a relevant NQF Level 7 qualification in Information Technology.

Applicants will be required to submit a portfolio of evidence, which may include:

- Academic records and prior learning achievements.
- Relevant professional or workplace experience.
- Evidence of technical capability in IT or cybersecurity-related areas.
- A motivation outlining readiness for further study.

Admission through RPL for access is granted only where sufficient evidence demonstrates the applicant's ability to succeed in a specialised, applied learning environment.

RPL for Credit (Advanced Standing)

In line with SAQA and institutional guidelines, a maximum of 50% of the total credits for the qualification may be awarded through RPL, where applicable and academically justifiable. RPL for credit may be considered where prior learning demonstrates clear alignment and content overlap with specific modules within the programme. This is typically limited to structured modules where equivalence in learning outcomes can be demonstrated.

Given the integrated and applied nature of the qualification:

- Credit recognition is evaluated on a module-by-module basis.
- Exemptions are granted only where there is sufficient evidence of depth and relevance.
- The Cybersecurity Risk Management Research Project must be completed in full to meet the qualification's exit level outcomes.

Assessment Process

All RPL applications are subject to a structured academic review process, which includes:

- Formal evaluation of the submitted portfolio of evidence.
- Assessment of alignment with programme learning outcomes and academic standards.
- Review and approval by the relevant institutional academic structures.

Admission through RPL is limited in accordance with institutional policy.

Application Process

Applications are submitted through the Belgium Campus iTversity online application portal. Applicants are required to submit standard admission documentation, together with additional supporting information to assess academic readiness and alignment with the programme.

Standard Documentation

Applicants must submit:

- A certified copy of identification documentation.
- A certified copy of full academic records.

BELGIUM CAMPUS iTversity

Additional Supporting Information

To support admission decisions, applicants may be required to submit:

- A brief motivation outlining their interest in cybersecurity and readiness for further study.
- Evidence of relevant technical knowledge, skills, or work experience (where applicable).
- For applicants applying through Recognition of Prior Learning (RPL), a portfolio of evidence will be required in line with the RPL process.

Selection Considerations

Admission is based on:

- Academic eligibility and prior qualifications.
- Alignment between the applicant's background and the technical requirements of the programme.
- Demonstrated readiness to engage with specialised cybersecurity content.
- Where applicable, RPL applications are evaluated through a structured academic process in line with institutional policy.

Programme Enquiries

For further information or academic enquiries regarding the Postgraduate Diploma in Cybersecurity
Risk Management, please contact:

Mr Francois Smit

Head of Department Networking & Cybersecurity

Belgium Campus iTversity

smit.f@belgiumcampus.ac.za