JINDAL GLOBAL BUSINESS SCHOOL
INDIA'S FIRST MULTI-DISCIPLINARY GLOBAL BUSINESS SCHOOL

O.P. Jindal Global University
A Private University Promoting Public Service
NAAC Accreditation - 'A' Grade

Jindal Global Business School
Course Outline

Course Title	Digital Risk, Cybersecurity, and Business Resilience
Core or Elective	Elective
Program and Batch	MBA-2025, IBM-2022, IBM-2023
Semester & Academic Year	Fall 2026
Credits	1.5
Discipline/Area	Information Systems and Analytics
Name of the Faculty Member/Course Instructor	Pramod Kumar Patnaik
Contact Details of the Faculty Member	Pramod.patnaik@jgu.edu.in
Contact Details of Support Staff	jgbs-eo@jgu.edu.in
Faculty Member's Open Office Day/s & Time	Monday 5.00 pm – 6.00 pm Wednesday 5.00 pm – 6.00 pm

Introduction to the Course

Digital risk refers to the potential threats and vulnerabilities that arise from the use of digital technologies in business operations, including cyberattacks, data breaches, system failures, and misuse of digital platforms. As organizations increasingly rely on digital systems, managing these risks has become a critical strategic priority. Cybersecurity plays a vital role in protecting information assets, ensuring data privacy, and maintaining the integrity and availability of digital systems. Business resilience, in this context, refers to an organization's ability to anticipate, withstand, respond to, and recover from digital disruptions while continuing to operate effectively.

In today's interconnected and technology-driven business environment, organizations face a wide range of cyber threats such as phishing attacks, ransomware, identity theft, and insider risks. These threats not only impact operational continuity but also damage organizational reputation and customer trust. Therefore, business management students need to understand the nature of digital risks and the importance of implementing robust cybersecurity frameworks and risk management strategies.

This course equips students with the knowledge and skills required to identify, assess, and mitigate digital risks in business settings. It emphasizes the integration of cybersecurity practices into business strategy and decision-

making processes. Students will learn how to safeguard digital assets, ensure compliance with data protection regulations, and develop incident response and business continuity plans. The course also highlights the role of human behavior, digital ethics, and governance in managing cybersecurity challenges.

Understanding digital risk and cybersecurity is not limited to IT professionals; it is equally important for business leaders who must make informed decisions regarding technology investments, risk management, and organizational resilience. This course prepares students to bridge the gap between technical and managerial perspectives, enabling them to contribute effectively to organizational security and resilience strategies. The course fosters critical thinking, problem-solving, and decision-making skills in the context of digital risk management. It encourages a proactive approach to identifying vulnerabilities and building resilient systems that can adapt to evolving threats. Students will also develop the ability to communicate cybersecurity risks and solutions to both technical and non-technical stakeholders.

This course is divided into three modules to provide a comprehensive understanding of digital risk, cybersecurity, and business resilience. The first module introduces the fundamentals of digital risk, types of cyber threats, and basic cybersecurity concepts. The second module focuses on risk management frameworks, data protection laws, governance mechanisms, and practical tools for securing digital systems. The final module explores business resilience strategies, including incident response planning, disaster recovery, and the role of emerging technologies in enhancing security. By the end of the course, students will be equipped not only to manage digital risks effectively but also to contribute to building resilient and secure business environments in an increasingly digital world.

Course Learning Objectives
At the end of the course, students should be able to

1. CLO1 - Explain the fundamental concepts of digital risk, cybersecurity, and business resilience, and their significance in modern business environments.

2. CLO2 - Identify and evaluate various types of cyber threats, vulnerabilities, and digital risks affecting organizations across industries.

3. CLO3 - Analyze the impact of cybersecurity incidents on business operations, reputation, and continuity, and assess appropriate risk mitigation strategies.

4. CLO4 - Develop strategies for implementing cybersecurity frameworks, data protection measures, and business continuity and disaster recovery plans.

5. CLO5 - Critically evaluate the ethical, legal, and regulatory implications of cybersecurity and digital risk management in organizational contexts.

Programme Competency Goals

MBA Programme Competency Goals (PCGs)		MBA Programme Learning Objectives (PLOs) Students will be able to
1	**Technological Agility:** Ability to adopt relevant technologies for better business decision making.	1. Understand relevant business technologies
		2. Understand future technologies in business domain
2	**Responsible Global Citizenship:** Ability to understand the interplay between local and global issues and to act with sensitivity towards ethical and social issues	3. Understand the interplay between local and global business issues
		4. Demonstrate sensitivity towards ethical issues
		5. Demonstrate sensitivity towards social issues
		6. Address societal issues
3	**Effective communication:** Ability to effectively exchange ideas and information	7. Present their ideas with clarity
		8. Prepare an organized and logical business document
		9. Use technology for effective communication
4	**Critical Thinking:** Ability to identify, analyze business problems and propose effective solutions	10. Identify main issues of business problems
		11. Examine information from different sources
		12. Draw inferences from analysis
		13. Evaluate alternatives
		14. Summarize and conclude
5	**Leadership:** Ability to take initiative, inspire and collaborate with others	15. Take initiative
		16. Contribute effectively in groups

PLO-PCG Assessments Mapping Matrix

Program Learning Objectives (PLOs)	**Program Competency Goals (PCGs)**	**Course Assessment Item**
This course helps you to develop the following Program Learning Outcomes:	This course helps you to develop the following Program Competency Goals:	This learning outcome will be assessed in the following items
PCG1-PLO1 PCG1-PLO2	PCG1	A1, A2, A3, A4, A5
PCG3- PLO7 PCG4- PLO10 PCG4- PLO12 PCG4- PLO13 PCG4- PLO14	PCG3, PCG4	A3, A4

Evaluation Schema

The course grade will be determined based on:

Assessment Task	**Weightage (Percentage)**	**Nature (Individual/Group)**	**Week of Assessment**	**PLOs to be Assessed**
A1 Class Participation	10%	Individual	All the sessions	PCG1- PLO1 PCG1- PLO2
A2 Quiz - Exercise	20%	Individual	6th and 12th Week	PCG1- PLO1 PCG1- PLO2
A3 Group Project- Proposal Stage	20%	Group	Week 3 (1 project proposal)	PCG1- PLO1 PCG1- PLO2 PCG4- PLO10 PCG4- PLO12 PCG4- PLO13
A4 Group Project- Final Presentation	20%	Group	Week 8 (1 final presentation)	PCG1- PLO1 PCG1- PLO2 PCG3- PLO7 PCG4- PLO10 PCG4- PLO12 PCG4- PLO13 PCG4- PLO14
A5 End term Examination	30%	Individual	Examination week	PCG1- PLO1 PCG1- PLO-2

Description of Assessments:

A1- Class participation: Students are evaluated on their level of involvement during class discussions and activities.

A2- The in-class quiz will be used to assess students' understanding of concepts covered in the class. There will be two MCQ quizzes in the 6th and 12th weeks of the course, conducted on UMS or pen and paper.

A3- Group Project – Proposal stage: The purpose the project is to provide students with in-depth hands-on experience of implementing digital transformation strategy for a selected business organization. The project requires the students to utilize the technical skills and knowledge acquired as part of the course.

A4- Group Project-Presentation: You are expected to carefully analyse a case study/business situation and present your analysis and findings in a PowerPoint/video format. The presentation/video must carry a thorough problem identification, analysis, and recommendation (probable solution, and action plan).

A5 End term examination- The end term examination will be of **30 marks of 1.5 hours duration**. This will be an invigilated exam according to the mode, modalities and process as decided by CoE.

Rubrics for Assessments

Grading Rubrics for the Presentation

Criteria	10 – Outstanding	9 – Proficient	8 – Basic	7 (or lower) - Below Expectations
OBJECTIVE				
Prepare and present the topic/case study as per the requirements	All portions of the assignment, including presentations, data, and details, were attempted and submitted. The presentation will be assessed based on the following. 1. Content quality (accuracy, depth, relevance) – 2 Marks 2. Organization (logical flow, clarity of structure) – 2 Marks 3. Delivery (confidence, clarity, eye contact, body language) – 2 Marks 4. Visual aids (appropriateness, design, effectiveness) – 2 Marks 5. Time management (adherence to time limits) – 1 Mark 6. Engagement (ability to hold audience interest, interaction) – 1 Mark			

Teaching Method

The course will have a judicious mix of lectures, storytelling, experiential exercises, and cases. Here the onus of learning will be with the student, and the instructor will be a facilitator. Instead of learning 'what to do', the cases will also be used as examples of real-world phenomena where issues arise, and good and bad practices are seen. The key to learning this way is to see many examples and situations and learn inductive as well as deductive ways from students' and managers' different experiences.

Textbook / Other Readings

Textbook:

- Whitman, M. E., & Mattord, H. J. *Management of Information Security*, 7th Edition, Publisher: Cengage Learning; ISBN-10: 0357506154; ISBN-13: 978-0357506158
- Textbook: Laudon, K. C., & Laudon, J. P. Management Information Systems: Managing the Digital Firm. 17th Edition, Publisher: Pearson Education; ISBN-10: 813178746X
- Von Solms, B., & van Niekerk, J. *Cybersecurity and Cyberwar: What Everyone Needs to Know*, 2nd Edition, Publisher: Oxford University Press; ISBN-10: 019090851X; ISBN-13: 9780190908515
- Calder, A., & Watkins, S. *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*, 7th Edition, Publisher: Kogan Page; ISBN-10: 1789668166; ISBN-13: 978-1789668162

- Herbane, B. *Business Continuity Management: Systems and Processes for Creating and Protecting Resilient Organizations*, 2nd Edition, Publisher: Routledge; ISBN-10: 1138199000; ISBN-13: 978-1138199002

Guest Speakers

Session	Faculty Name	Guest Speaker	Title of the Session
10th	Pramod Kumar Patnaik	Bhanu Prashant	Digital Risk and Cybersecurity

Session Plan

Session Details	Topics	PLOs Covered
Session 1	Introduction to digital risk, cybersecurity, and business resilience	PLO1 and PLO2
Objective of the session	To build a foundational understanding of digital risk, cybersecurity concepts, and their importance in modern business environments.	
Subtopics to be covered	· Meaning and Scope of Digital Risk · Introduction to Cybersecurity · Types of Cyber Threats (Phishing, Malware, Ransomware) · Importance of Cybersecurity in Business	
Readings	Chapter 1 from TB1	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 2	Cyber Threat Landscape and Attack Vectors	PLO1 and PLO2
Objective of the session	To examine different types of cyber threats and understand how organizations are targeted through various attack vectors.	
Subtopics to be covered	. Cyber Threat Actors (Hackers, Insider Threats, Nation States) · Attack Vectors and Vulnerabilities · Case Examples of Cyber Attacks · Threat Intelligence Basics	
Readings	Chapter 1 from TB1	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 3	Information Security Principles and Framework	PLO1 and PLO2
Objective of the session	To understand core principles of information security and standard cybersecurity frameworks used in organizations.	
Subtopics to be covered	· CIA Triad (Confidentiality, Integrity, Availability) · Risk, Threat, Vulnerability Concepts · Overview of ISO 27001, NIST Framework · Security Controls and Policies	
Readings	Chapter 4 from TB1	

Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 4	Risk Assessment and Risk Management in Digital Systems	PLO1 and PLO2
Objective of the session	To analyze how organizations identify, assess, and prioritize digital risks.	
Subtopics to be covered	· Risk Identification and Classification · Risk Assessment Techniques · Qualitative vs Quantitative Risk Analysis · Risk Mitigation Strategies	
Readings	Chapter 4 from TB1	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 5	Data Protection, Privacy, and Legal Frameworks	PLO1 and PLO2
Objective of the session	To understand data protection laws and ethical responsibilities in handling digital data.	
Subtopics to be covered	· Data Privacy Concepts · Overview of IT Act, GDPR basics · Data Protection Principles · Ethical Issues in Data Usage	
Readings	Chapter 8 from TB2	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 6	Cybersecurity Governance and Organizational Strategy	PLO1 and PLO2
Objective of the session	To explore how cybersecurity is integrated into business strategy and governance structures.	
Subtopics to be covered	· Cybersecurity Governance Models · Role of Leadership in Cybersecurity · Security Policies and Compliance · Risk Culture in Organizations	
Readings	Chapter 8 from TB2	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 7	Human Factors and Social Engineering in Cybersecurity	PLO1 and PLO2
Objective of the session	To examine the role of human behavior in cybersecurity risks and attacks.	
Subtopics to be covered	· Social Engineering Attacks · Phishing and Behavioral Exploits · Insider Threats · Building Security Awareness	
Readings	Chapter 11 from TB1	

Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 8	Cybersecurity Technologies and Tools	PLO1 and PLO2
Objective of the session	To understand key technologies used to protect organizational systems and data.	
Subtopics to be covered	· Firewalls, IDS/IPS · Encryption Basics · Authentication Mechanisms (MFA) · Endpoint and Network Security	
Readings	Chapter 8 from TB2	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 9	Incident Response and Crisis Management	PLO1 and PLO2
Objective of the session	To develop an understanding of how organizations respond to cybersecurity incidents.	
Subtopics to be covered	· Incident Response Lifecycle · Detection and Containment · Recovery Strategies · Crisis Communication	
Readings	Chapter 4 from TB1	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 10	Guest Lecture / Industry Session	PCG1- PLO1 PCG1- PLO2 PCG4- PLO10 PCG4- PLO12
Objective of the session	To provide industry insights into real-world cybersecurity challenges and practices.	
Subtopics to be covered	· Real-world Cyber Incidents · Industry Best Practices	
Readings	NA	
Case Title & Number	NA	
Pedagogy	Lecture-based discussion	
Session 11	Business Continuity and Disaster Recovery Planning	PLO1 and PLO2
Objective of the session	To understand how organizations ensure continuity during disruptions.	
Subtopics to be covered	· Business Continuity Planning (BCP) · Disaster Recovery (DR) · Resilience Frameworks	
Readings	Chapter 12 from TB1	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	

Session 12	Emerging Risks: AI, Cloud, and Digital Platforms	PLO1 and PLO2
Objective of the session	To evaluate risks associated with emerging technologies.	
Subtopics to be covered	· AI Risks and Bias · Cloud Security Risks · Platform Economy Risks · Third-party Risks	
Readings	Pre-read: Chapter 8 from TB2	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 13	Measuring Cyber Risk and Organizational Resilience	PLO1 and PLO2
Objective of the session	To assess how organizations measure and improve cybersecurity performance.	
Subtopics to be covered	· Cyber Risk Metrics and KPIs · ROI of Cybersecurity Investments · Resilience Assessment	
Readings	Chapter 5 from TB1	
Case Title & Number	NA	
Pedagogy	Lectures, cases, and class discussions	
Session 14	Group presentation	PCG1- PLO1 PCG1- PLO2 PCG3- PLO7 PCG4- PLO10 PCG4- PLO12 PCG4- PLO13 PCG4- PLO14
Objective of the session	Group assignments presentations and course wrap-up	
Subtopics to be covered	NA	
Readings	NA	
Case Title & Number	NA	
Pedagogy	Reflection and student group presentation	
Session 15	Reading & Revision Week/ Examination Week*	PLO1 and PLO2
Objective of the session	NA	
Subtopics to be covered	NA	
Readings	NA	
Case Title & Number	NA	
Pedagogy	NA	

*Elective Endterm Examinations may take place in the last week of classes.

Disability Support

JGU endeavours to make all its courses accessible to students. The Disability Support Committee (DSC) has identified conditions that could hinder a student's overall wellbeing. These include physical and mobility-related difficulties, visual impairment, hearing impairment, mental health conditions, and intellectual/learning difficulties, e.g., dyslexia and dyscalculia. Students with any known disability needing academic and other support are required to register with the Disability Support Committee (DSC) by following the procedure specified at **https://jgu.edu.in/disability-support-committee/**

Students who need support may register any time during the semester up until a month before the end semester exam begins. Those students who wish to continue receiving support from the previous semester, must re-register within the first month of a semester. Last-minute registrations and support might not be possible as sufficient time is required to make the arrangements for support.

The DSC maintains strict confidentiality about the identity of the student and the nature of their disability and the same is requested from faculty members and staff as well. The DSC takes a strong stance against in-class and out-of-class references made about a student's disability without their consent and disrespectful comments referring to a student's disability.

All general queries are to be addressed to **disabilitysupportcommittee@jgu.edu.in**

Disclaimer: This course outline including assessments, mode, nature and weightage of assessments, sessions, sequence of sessions and/or readings may be revised during the semester if such need arises.