DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

in association with
DREW & NAPIER

Agentic AI Risk Assessment

Course Objectives

‘Agentic AI’ is currently hailed as the next big thing to the digital transformation of work, life, and learning. Such systems tend to be based on the popular and successful, though quite diverse, GenAI and Large Language Models. Due to their reliance on other technologies, their automated communication and coordination, and in growing cases even delegated / autonomous actions, they bring their own set of new, pressing and peculiar risks and threats to security, identity management, privacy and data protection. This course introduces and explores local and international Agentic AI specific risk assessment approaches, guidelines and frameworks through theoretical foundations, practical considerations, and risk-assessment demos. This equips the audience with a solid basis on the various evolving approaches to be able to customise a suitable approach for their organisation. This course brings clarity, context, and meaning to the growing and still consolidating field, from an engineering, factual point of view. This is critical for an audience in charge of governance, strategies, and decision making around Agentic AI, as technology-based risk management is ideally built upon a meaningful and realistic risk assessment that includes technological aspects.

This course complements our What to look out for when procuring an AI Solution - Legal and Technology Essentials course and our Deep Learning Essentials course. It requires a basic understanding of this fast-evolving technology, as provided in our course Agentic AI Primer.

Who should attend?

- AI professionals, Risk & Compliance Professionals Data Protection Officers (DPOs)
- Privacy / Software Engineers, Technical Staff, Developers, Data Analysts, Data Architects, and Project / Risk Managers
- Executives, Managers, and Staff involved in the management, procurement, development, test, or deployment of Agentic AI systems

Course Details

Course Code:	AI202
Title:	Agentic AI Risk Assessment
Duration:	½ day (approximately 3.5 contact hours)
Mode of Training:	In-person
Venue:	Drew & Napier LLC 10 Collyer Quay, 10th Floor, Ocean Financial Centre Singapore 049315
Course Fee:	S$400.00 (excluding GST)

To view available dates and register for this course, please click here. You may also register for this course and view all available courses on our course schedule page (www.drewnapier.com/Academy/Course-Schedule-Ors).

Course Outline

- **Risk Related Key Terminology for AI and Agentic AI**

- **Agentic AI Risk Assessment foundations**
  - Architecture (Agents versus Applications)
  - Risk, Issue, Problem Zone
  - Threat Modelling

- **Details and Demo on Guidelines and References**
  - *Agentic Risk & Capability Framework* (ARC)
  - Cyber Security Agency of Singapore (CSA)'s *Securing Agentic AI*
  - Infocomm Media Development Authority (IMDA)'s *Model AI Governance Framework for Agentic AI*
  - Open Worldwide Application Security Project (OWASP) Top 10

Course Facilitator

Albert Pichlmaier is Senior Learning Technology Designer with Drew Academy and concurrently Senior Cybersecurity & Privacy Engineer with Drew & Napier's Data Protection, Privacy & Cybersecurity practice. He holds a degree in Computer Science from a German tertiary institution. He is a Certified Artificial Intelligence Governance Professional (AIGP), a Certified Information Systems Security Professional (CISSP), a Certified Data Privacy Solutions Engineer (CDPSE), a holder of the Singapore WSQ Advanced Certificate in Learning and Performance (ACLP), and a certified Blockchain Developer. Albert is credited as an inventor of two patents (one involving AI technology) granted in Germany and other countries. His technical expertise covers a wide-ranging area of matters involving Cybersecurity, Privacy Engineering, Cryptography, Quantum Computing, Artificial Intelligence / Machine Learning, Blockchain Development, Data Analytics, Big Data, and Data Visualisation. For the courses and webinars under the Drew Academy, he draws from this pool of knowledge and experience to explain technical content to non-technical audiences, develop proof-of-concept and learning tools, and engage with experts on finer details.

Albert was formerly an Executive Manager with the Personal Data Protection Commission (PDPC), where he was involved in technology assessments for data breach investigations, research into trending / disruptive technologies and advising on technical aspects of various PDPC guidelines and publications (amongst other matters). Prior to his role with the PDPC, Albert worked in technology-related organisations in the private and public sector in Germany, Spain, and Singapore. He was also a technopreneur, having set up a company to provide testing tools for embedded systems and smartcard applications.