THE UNIVERSITY OF BRITISH COLUMBIA

School of Information
Faculty of Arts

We acknowledge that we are on the traditional, ancestral and unceded territory of the hən̓q̓əmin̓əm̓ speaking Musqueam people.

iSchool Mission: Through innovative research, education and design, our mission is to enhance humanity's capacity to engage information in effective, creative and diverse ways.

ARST 575J/LIBR 514K – IT Security, Information Assurance, and Risk Management– Course Syllabus (3)

Program:	Master of Archival Studies/ Master in Library and Information Science
Year:	**2022-2023, WT 2**
Course Schedule:	**Wednesdays, 9-12 am**
Location:	**Leo and Thea Koerner University Centre, room 101** **https://learningspaces.ubc.ca/buildings/leon-and-thea-koerner-university-centre-ucen**
Instructor:	**Danielle Alves Batista**
Office location:	iSchool Adjunct Office, IBLC, room
Office phone:	**(604) 783-1732**
Office hours:	**Tuesdays and Thursdays, 1-2 pm PT**
E-mail address:	**danielle.batista@ubc.ca**
Learning Management Site:	

Calendar Description: Course developed to bring students to a position in which they can identify threats and vulnerabilities to information assets and provide organizations with controls to guarantee information assurance.

Course Overview: In the digital era, records and information are being created and kept using a wide variety of digital technologies – web- and mobile-based user interfaces, databases, cloud, blockchain – running over the Internet. This has exposed records and information to new risks and introduced unprecedented challenges for records and information professionals charged with the management and long-term preservation of authentic records and information. In response, records and information professionals must learn new knowledge and skills in order to promote information security and assurance.
This course therefore provides an overview of the fields of IT Security, Information Assurance and Risk Management. IT Security and Information Assurance are concerned with threats to the Confidentiality, Integrity and Availability (CIA) of information systems. Risk management comprises a set of coordinated activities to direct and control an organization about risk. This course will explore how IT Security, Information Assurance, and Risk Management intersect with the management of records and information in digital environments and will address the application of IT Security, Information Assurance and Risk Management theories, principles, and techniques to the management of records and information-related risks.

Learning Outcomes:

Upon completion of this course students will be able to:

1. Articulate and critically reflect upon the history and development of the fields of IT Security, Information Assurance and Risk Management and appreciate the differences between the three fields [MLIS: 4.1, 5.1, 5.2, 5.3] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2].

2. Fluently articulate and apply Information Assurance and Risk Management concepts and terms [MLIS: 4.1] [MAS: 1.4, 4.2]
3. Articulate and critically evaluate Security Management and Information Assurance practices [MLIS: 4.1, 5.1, 5.2, 5,3] [MAS: 1.4, 4.2]
4. Understand Risk Management practices and critically reflect upon how they can be applied to managing records and information-related risks [MLIS: 1.1, 1.3, 3.2, 5.1, 5.2, 5.3] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2]
5. Articulate Access control practices and critically evaluate how they can be applied to managing records and information-related risks [MLIS: 1.1, 1.3, 3.2] [MAS: 1.1, 1.2, 1.3, 1.4, 1.5]
6. Articulate and critically evaluate Telecommunications and Network Technologies, risks to records and information arising from these technologies, and ways in which these risks may be managed [MLIS: 1.1, 1.3, 3.2] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2].
7. Articulate and critically evaluate the Application Technologies and the Application Development Life Cycle, risks to records and information arising from these technologies and ways in which these risks may be managed [MLIS: 1.1, 1.3, 3.2] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2].
8. Articulate and critically evaluate Business Continuity and Disaster Planning practices and how these may be used to address risks to records and information [MLIS 1.1, 1.3, 3.2] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2]
9. Articulate and critically evaluate Physical Security practices and how these may be used to address risks to records and information [MLIS 1.1, 1.3, 3.2] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2].
10. Articulate and critically discuss recent technology trends (e.g. Cloud Computing, Social Networking and Mobile Technologies, the risks to records and information to which these technologies may give rise, and ways in which these risks may be managed [MLIS 1.1, 1.3, 3.2] [MAS: 1.1, 1.2, 1.4, 1.5, 4.2]

Course Topics:

- History and development of the fields of IT Security, Information Assurance and Risk Management and appreciate the differences between the three approaches.
- IT Security, Information Assurance and Risk Management concepts and terms.
- Security Management and Information Assurance practices.
- Risk Management practices and how they can be applied to managing records and information related risks.
- Telecommunications and Network Technologies, risks to records arising from these technologies and ways in which these risks may be managed.
- Application Technologies and the Application Development Life Cycle, risks to records and information arising from these technologies and ways in which these risks may be managed.
- Access Control.
- Business Continuity and Disaster Planning practices and how these may be used to address risks to records and information.
- Physical Security practices and how these may be used to address risks to records and information.
- Technology trends (e.g. Cloud Computing, Social Networking and Mobile Technologies), the risks to records and information to which these technologies may give rise, and ways in which these risks may be managed.

Prerequisites:

MAS and Dual Students: completion of the MAS core courses

MLIS students: LIBR 516 and completion of the MLIS core courses, plus permission of the SLAIS Graduate Adviser.

Format of the course: In person lectures, in-class exercises, weekly quizzes, one poster presentation and a final project.

Required and Recommended Reading:

Required:

The course textbook is Stewart, James M., Chapple, Mike, and Gibson, Darril (2012). *CISSP: Certified Information Systems Security Professional Study Guide: Certified Information Systems Security Professional Study Guide,* Sixth Edition. NY, NY: John Wiley & Sons. Available online from the UBC Library: https://ebookcentral.proquest.com/lib/ubc/detail.action?docID=875861

Recommended: recommended readings are distributed on a weekly basis.

Readings [week by week]:

January 11 – Introduction to the course

No required readings

January 18 – IT Security, Information Assurance and Risk Management Perspectives and Standards

Required

International Standards Organization. (2016). ISO/IEC 27000:2016 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva, Switzerland: International Organization for Standardization (ISO).

International Standards Organization. (2014). ISO/TR 18128:2014–Information and documentation – Risk management for records processes and systems. Geneva, Switzerland: International Standards Organization (ISO). Available

Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapters 3 & 5. In CISSP: Certified information systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended

Donaldson, D. R., & Bell, L. (2018). Security, Archivists, and Digital Collections. Journal of Archival

Organization, 15(1-2), 1-19.

Enns, L. (2016, December). Protecting information assets using ISO/IEC security standards. Information Management Magazine. Available online through the UBC Library system.

International Standards Organization. (2013). ISO/IEC 27001:2013–Information technology–Security techniques–Information security management systems –Requirements. Geneva, Switzerland: International Standards Organization (ISO).

January 25 – Application & Presentation Layer Attacks & Risk Mitigation Strategies, etc.

Required

Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapters 1, 2, 7, and 8. In CISSP: Certified information

systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended

Aitel, D. (n.d.). The hacker strategy. Available at: http://www.immunityinc.com/downloads/DaveAitel_TheHackerStrategy.pdf.

Barth, A., Jackson, C., Reis, C,.& The Google Chrome Team. (2008) The security architecture of the Chomium browser. Available at: https://seclab.stanford.edu/websec/chromium/chromium-securityarchitecture.pdf.

Brose, G. (2011). Access control. In van Tilborg, H. C. A., & Jajodia, S. (Eds), Encyclopedia of Cryptography and Security (pp.2-7). Berlin: Springer.

Cowan, C., & Beatti, S. (1999). Buffer overflows: Attacks and defenses for the vulnerability of the decade. Proceedings of DARPA Information Survivability Conference and Expo (DISCEX). Available at: https://cis.upenn.edu/~sga001/classes/cis331f19/resources/buffer-overflows.pdf.

De Capitani di Vimercati, S. (2011). Access control policies, models and mechanisms. In van Tilborg,

H. C. A., & Jajodia, S. (Eds), Encyclopedia of Cryptography and Security (pp.13-14). Berlin: Springer.

D-CENT. (2013). Research on identity ecosystem. Available at: http://dcentproject.eu/wpcontent/uploads/2015/08/D3.3-Research-on-Identity-Ecosystem_part1.pdf.

Identity Ecosystem Steering Group (IDESG). (n.d.). Available at: https://www.idesg.org.

International Standards Organization. (2011). ISO/IEC 27034:2011 – Information technology – Se curitytechniques –Application security–Part 1: Overview and concepts. Geneva, Switzerland: International Organization for Standardization (ISO).

Jaeger, T. (2008). Chapter 4. In Operating systems security. San Rafael, CA: Morgan & Claypool Publishers.

Jarzombek, J. (2012). Software assurance: Enabling security and resilience through software lifecycle. Available at: http://csrc.nist.gov/groups/SMA/forum/documents/october-2012_fcsm-jjarzombek.pdf.

Kissel, R., et al. Security considerations in the system development life cycle. (2008). Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf.

Maller, E., & Drummond, R. (2008). The Venn of identity management. IEEE Security & Privacy, 6(2), 16–23. Available at: https://css.csail.mit.edu/6.858/2012/readings/identity.pdf

Mitre Corporation. (2007, 2015). CAPEC - Common attack pattern, enumeration and classification (CAPEC). Available at: https://capec.mitre.org/

Mougoue, Ernest. (2016). SSDLC 101: What Is the secure software development life cycle? Available at: https://dzone.com/articles/ssdlc-101-what-is-the-secure-software-development

National Institute of Standards and Technology Computer Security Division. (2012). NIST Special Publication 800-30: Guide for Conducting Risk Assessments (No. NIST SP 800-30r1). Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (see Appendices D-F).

Open Web Application Security Project (OWASP). Available at: https://www.owasp.org/index.php/Main_Page

Open Web Application Security Project (OWASP): Secure SDLC cheat sheet. Available at: https://www.owasp.org/index.php/Main_Page.

Sotirov, A., & Dowd, M. (2008). Bypassing browser memory protections: Setting back browser security by 10 years. Proceedings of Black Hat USA 2008 Briefings and Training. Available at: http://www.blackhat.com/presentations/bh-usa-08/Sotirov_Dowd/bh08-sotirov-dowd.pdf.

Shostock, A. (2014). Elevation of privilege: Drawing developers into threat modelling. Presented at the 2014 USENIX Summit on Gaming, Games and Gamification in Security Education. Available at: https://www.usenix.org/node/184967

The White House. (2011). National strategy for trusted identities in cyberspace. Washington, DC: The White House. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

February 1 – Telecommunications and Network Attacks and Risk Mitigation Strategies, Part I

Required

Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapters 3 & 4. In CISSP: Certified information systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended

de Oliveira Albuquerque, R., et al. (2014). A layered trust information security architecture. Sensors,

14(12), 22754-22772.

DeSoete, M. (2011). Security architecture. In van Tilborg, H. C. A., & Jajodia, S. (Eds), Encyclopedia of cryptography and security (p. 1144). Berlin: Springer.

Barth, A., Jackson, C., & Mitchell, J. C. (2009). Securing frame communication in browsers. In Communications of the ACM, 52(6), 83-91. Available at: http://seclab.stanford.edu/websec/frames/postmessage.pdf.

Mitre Corporation. (2007, 2015). CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC). Available at: https://capec.mitre.org/.

Ramachandran, J. (2002). Designing security architecture solutions. New York: Wiley.

Stonebruner, G., Hayden, C., & Feringa, A. (2004). Engineering principles for information technology security (A baseline for achieving security), Revision A. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf.

Ross, R., McEvilley, M., & Oren, J.C. (2016). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

February 8 – Telecommunications and Network Attacks and Risk Mitigation Strategies, Part II

Required:

Bardwaj, A., & Gounder, S. (2017, November). Security challenges for cloud-based email infrastructure. In Network Security, 8-15. Available in the Canvas module folder.

Filippo, L. (2017, December). How to footprint, report, and remotely secure compromised IoT devices. In Network Security, 10-15. Available in the Canvas module folder.

Recommended:

Barth, A., Jackson, C., & Mitchell, J. C. (2009). Securing frame communication in browsers. In Communications of the ACM, 52(6), 83-91. Available at: http://seclab.stanford.edu/websec/frames/postmessage.pdf.

de Oliveira Albuquerque, R., et al. (2014). A layered trust information security architecture. Sensors, 14(12), 22754-22772.

DeSoete, M. (2011). Security architecture. In van Tilborg, H. C. A., & Jajodia, S. (Eds), Encyclopedia of cryptography and security (p. 1144). Berlin: Springer.

Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. Computer Law & Security Review, 28(5), 522-531.

Mitre Corporation. (2007, 2015). CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC). Available at: CAPEC website: https://capec.mitre.org/.

O'Hare, B. T., & Malisow, B. (2017). CCSP® (ISC)2® Certified cloud security professional: Official study guide. New York: John Wiley & Sons.

Ramachandran, J. (2002). Designing security architecture solutions. New York: Wiley.

Stuart, K., & Bromage, D. (2010). Current state of play: records management and the cloud. Records Management Journal, 20(2), 217-225.

Stonebruner, G., Hayden, C., & Feringa, A. (2004). Engineering principles for information technology security (A baseline for achieving security), Revision A. Gaithersburg, MD: National institute of standards and technology. Available at: https://csrc.nist.gov/publications/detail/sp/800-27/reva/archive/2004-06-21

February 15 – Cryptography

Required:
Lemieux, V. L. (2016). Trusting records: Is Blockchain technology the answer?. Records Management Journal 26(2), 110-139.
Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapters 9 & 10. In CISSP: Certified information systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended:

Batista, D. and Lemieux, V.L. (2019). Bounded and shielded: Assessing security aspects and trustworthiness of smart contracts. Proceedings of the Annual Conference of the Canadian Association for Information Science, June 4, 2019, University of Alberta Libraries. Available at: https://journals.library.ualberta.ca/ojs.cais-acsi.ca/index.php/cais-asci/article/view/1063/947

Blanchette, J-F. (2012). Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents. Boston, MA: The MIT Press.

Bonneau, J,. Miller, A. Clark, J., Narayanan, A., Kroll, J., & Felten, E.W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Presented at IEEE SSP 2015. Available at: http://users.encs.concordia.ca/%7Eclark/papers/2015_sp.pdf

Casey, M. J., & Vigna, P. (2018). Chapter 1. In The truth machine: The Blockchain and the future of everything (pp. 17-35). St. Marten's Press.

Eskandari, S., Barrera, D., Stobert, E., & Clark, J. A. (2015). First Look at the Usability of Bitcoin Key Management. Presented at USEC 2015, San Diego, CA. Available at: https://arxiv.org/pdf/1802.04351.pdf .

Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. A. (2019). The margin between the edge of the world and infinite possibility: Blockchain, GDPR and information governance. Records Management Journal, 29(1/2), 240-257.

Koren, I. (2016). Introduction to crytography. University of Massachusetts, Dept. of Electrical Engineering. Available at: http://euler.ecs.umass.edu/ece597/pdf/Crypto-Part1-intro.pdf.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.

February 22 – Winter Session Term 2 midterm break - Reading week

March 1 – Risk Management, Part I

Required:

Green, E. B. Green & Solander, A. (2015, June 17). Privacy & Security Crash Course: How Do I Execute a Risk Mitigation Plan?. Available at: https://www.youtube.com/watch?v=_EHOf0Nbauw&t=11s.

Lemieux, V. L. (2010). The records-risk nexus: Exploring the relationship between records and risk. Records Management Journal 20(2), 199-216.

Recommended:

International Standards Organization. (2014). ISO/TR 18128:2014–Information and documentation – Risk assessment for records processes and systems. Geneva, Switzerland: International Standards Organization (ISO). Available in Canvas module folder.

Lemieux, V. L. Managing risks for records and information. (2004). Presented at ARMA International 2004.

Lemieux, V. L. (2014). Risk & Opportunity: Risk to Records. Available at: https://www.youtube.com/watch?v=yaDquOVW2RM.

Lemieux, V. L. (2004). Two approaches to managing information risks. Information Management (38)5, 56. Available online through the UBC Library system.

March 8 – Risk Management, Part II

Required:

Computer Security Division. (2012). NIST Special Publication 800-30: Guide for conducting risk assessments (No. NIST SP 800-30r1). Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapter 6. In CISSP: Certified information systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended:

Lemieux, V. L. Managing risks for records and information. (2004). Presented at ARMA International 2004.

Lemieux, V. L. (2014). Risk & Opportunity: Risk to Records. Available at: https://www.youtube.com/watch?v=yaDquOVW2RM.

Lemieux, V. L. (2004). Two approaches to managing information risks. Information Management (38)5, 56. Available online through the UBC Library system.

March 15 – Security Operations & Incident Response Management

Required:

Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapters 13 & 14. In CISSP: Certified information systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended:

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security incident handling guide: recommendations of the National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Electric Power Research Institute. (2013). Guidelines for planning an integrated security operations center. Available at: https://www.smart-energy.com/wp-content/uploads/2014/02/EPRI-Planning-ISOCreport.pdf.

Building a Security Operations Center (SOC). (n.d.). Available at: https://cybersecurity.att.com/solutions/security-operations-center/building-a-soc

Kowtha, S., Nolan, L.A., & Daley, R.A. (2012). Cyber security operations center characterization model and analysis. In IEEE 2012 Conference on Technologies for Homeland Security (HST) (pp. 470,475, 13-15).

McAfee® Foundstone® Professional Services. Creating and maintaining a SOC: The details behind successful Security Operations Centers. Available at: https://communitym.trellix.com/nysyc36988/attachments/nysyc36988/siem/7399/1/wp-creating-maintaining-soc.pdf

Wei, D., Lu, Y., Jafari, M., Skare, P., & Rohde, K. (2010, Jan). An integrated security system of protecting Smart Grid against cyber attacks. Innovative Smart Grid Technologies (ISGT), (1)7, 19-21.

March 22 – IT Security, Information Assurance and Risk Management Policy Issues in Society

Required:

Stewart, James Michael, Chapple, Mike, and Gibson, Darril. CISSP: Certified Information Systems Security Professional Study Guide. 6th Ed. Indianapolis: John Wiley & Sons, 2012. Chp. 18.

Recommended:

Allhoff, F., Henschke, A., & Strawser, B. J. eds. (2016). Binary bullets: The ethics of cyberwarfare. Oxford University Press.

Lonsdale, D. J. (201). Warfighting for cyber deterrence: A strategic and moral imperative. Philosophy & Technology, 31(3), 409-429.

Moore, A. D. (2016). Privacy, Security and accountability: ethics, law and policy. New York: New York: Rowman & Littlefield.

Neal, P. 2019. Protecting the information society: exploring corporate decision makers' attitudes towards active cyber defence as an online deterrence option. PhD Diss. Royal Roads University. https://viurrspace.ca/handle/10613/11119

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. New York. Broadway Books.

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. Ethics and Information Technology, 20(2), 127-142.

March 29 – Business Continuity and Disaster Recovery, etc.

Required:

Stewart, J. M., Chapple, M., & Gibson, D. (2012). Chapters 15, 16 & 17. In CISSP: Certified information systems security professional study guide (6th ed.). Indianapolis: John Wiley & Sons.

Recommended:

California Department of General Services, Records & Information Management. (2003). Vital records protection and disaster recovery handbook. Sacramento, CA: State of California. Available at: https://silo.tips/download/vital-records-protection-and-disaster-recovery-handbook.

Jones, V. (2011). How to avoid disaster: RIM's crucial role in business continuity planning. Information Management (45),6, 36-47. Available online through UBC Library.

Rike, B. (2003). Prepared or not . . . that is the vital question. Information Management Journal (37),3, 25-33. Available online through UBC Library.

April 5 – IT Security, Information Assurance and Risk Management Training and Awareness

Required:

McIlwraith, A. (2016). Chapter 1-3. In Information security and employee behaviour: How to reduce risk through employee education, training and awareness. Routledge.

Tseng, S.-S., Yang, T.-Y., Wang, Y.-J., & Lu, A.-C. (n.d.). Designing a cybersecurity board game based on design thinking approach. In L. Barolli, F. Xhafa, N. Jaraid, & T. Enokido (Eds.), International conference on innovative mobile and internet services in ubiquitous computing (pp. 642–650). Springer, Cham.

Recommended:

Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. (2006, May) Cyber security training and awareness through game play. In IFIP International Information Security Conference (pp. 431-436). Boston, MA: Springer.

Yang, C. C., Tseng, S. S., Lee, T. J., Weng, J. F., & Chen, K. (2012, July).. Building an anti-phishing game to enhance network security literacy learning. In 2012 IEEE 12th International Conference on Advanced Learning Technologies (pp. 121-123).

Course Assignments and Assessment

Assignment Name	Due Date	Weight	Comments	Graduate Competencies
Module Quizzes (weekly online and available on Canvas)	Throughout	30%	Each quiz is worth 10 points. Final results will be scaled to comprise 30% of the final grade.	MLIS: 1.1, 1.2,1.4, 1.5, 3.2 MAS: 1.1, 1.2, 1.4, 1.5, 4.2
Weekly activities – poster presentation	Throughout	30%	Each presentation is worth 30% of the final grade.	MLIS: 1.1, 1.2, 1.4, 1.6, 2.1, 2.3, 3.1.2, 4.1, 5.1, 5.2, 5.3

				MAS: 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 4.2
Final project – Risk Assessment Assignment	April 13	40%	Details available on Canvas	MLIS: 1.1, 1.2, 1.4, 1.6, 2.1, 2.3, 3.1.2, 4.1, 5.1, 5.2, 5.3 MAS: 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 4.2

Course Schedule [week-by-week]:

Topic	**Date**
• Introduction to instructor • Introduction to the course • Introduction to IT Security, Information Assurance and Risk Management and their relationship to records and archives administration	Week 1 (Jan. 11)
• IT Security and Risk Management Perspectives and Standards • Information Security Governance and Risk Management • The Open Systems Interconnection Model Complete Required Readings for the week Complete Module 1 Quiz in Canvas Week 2 Presentations	Week 2 (Jan. 18)
• Application & Presentation Layer Attacks and Risk Mitigation Strategies • Access Control • Secure Software Development Complete Required Readings for the week Complete Module 2 Quiz in Canvas Week 3 Presentations	Week 3 (Jan. 25)
Telecommunications and Network Attacks and Risk Mitigation Strategies, Part I Complete Required Readings for the week Complete Module 3 Quiz in Canvas Week 4 Presentations	Week 4 (Feb. 1)
Telecommunications and Network Attacks and Risk Mitigation Strategies, Part 2 Complete Required Readings for the week Complete Module Quiz in Canvas Week 5 Presentations	Week 5 (Feb. 8)
• Cryptography • Blockchain Complete Required Readings for the week Complete Module Quiz in Canvas Week 6 Presentations	Week 6 (Feb. 15)
Winter Term 2 Break	Reading week (Feb. 22)
• Risk Management, Part I Complete Required Readings for the week	Week 7 (March 1)

Complete Module Quiz in Canvas Week 7 Presentations	
• Risk Management, Part II Complete Required Readings for the week Research and submit target system for Risk Assessment Assignment to instructor for approval Week 8 Presentations	Week 8 (March 8)
• Security Operations • Incident Response Management Complete Required Readings for the week Complete Module Quiz in Canvas Week 9 Presentations	Week 9 (March 15)
• IT Security, Information Assurance and Risk Management Policy Issues in Society ! Fake news ! Privacy vs. Security ! Active Defense ! BYOD ! Remote working Complete Required Readings for the week Complete Module Quiz in Canvas Week 10 Presentations	Week 10 (March 22)
• Physical Security • Business continuity and disaster recovery Complete Required Readings for the week Complete Module Quiz in Canvas Week 11 Presentations	Week 11 (March 29)
• The human factor in IT Security • IT Security, Information Assurance and Risk Management Training and Awareness • Building a career in IT Security, Information Assurance and Risk Management Complete Required Readings for the week Discussions about the final assignment. **RISK ASSESSSMENT ASSIGNMENT DUE BY April. 13**	Week 12 (April 5)

Attendance: Up to 3 excused absences are allowed with prior notification to me. Additional absences will require a note from a health professional or Centre for Accessibility. Failure to provide this documentation could result in a lower course mark.

Evaluation: All assignments will be marked using the evaluative criteria given on the iSchool web site and, more specifically, in accordance with assignment grading rubrics. Assignments will be regraded only in exceptional circumstances. Missed assignments will be dealt with according to the policy outlined under academic concessions (below).

Required Materials: Students will need a stable internet connection, and access to UBC's Canvas system. Students should ensure that they have registered to receive communications via Canvas.

Academic Concession: Students who miss marked coursework for the first time (assignment, exam, presentation, participation in class) and the course is still in-progress, should **speak with the instructor immediately** to find a solution for missed coursework. If you miss marked coursework (assignment, exam, presentation, participation in class) and are an Arts student, review the Faculty of Arts' academic concession page and then complete Arts Academic Advising's online academic concession form, so that an advisor can evaluate your concession case. If you are a student in a different Faculty, please consult your Faculty's webpage on academic concession, and then contact me where appropriate.

Policies and Resources to Support Student Success: UBC provides resources to support student learning and to maintain healthy lifestyles but recognizes that sometimes crises arise and so there are additional resources to access including those for survivors of sexual violence. UBC values respect for the person and ideas of all members of the academic community. Harassment and discrimination are not tolerated nor is suppression of academic freedom. UBC provides appropriate accommodation for students with disabilities and for religious and cultural observances. UBC values academic honesty and students are expected to acknowledge the ideas generated by others and to uphold the highest academic standards in all of their actions. Details of the policies and how to access support are available here (https://senate.ubc.ca/policies-resources-support-student-success)

Academic Integrity: The academic enterprise is founded on honesty, civility, and integrity. As members of this enterprise, all students are expected to know, understand, and follow the codes of conduct regarding academic integrity. At the most basic level, this means submitting only original work done by you and acknowledging all sources of information or ideas and attributing them to others as required. This also means you should not cheat, copy, or mislead others about what is your work. Violations of academic integrity (i.e., misconduct) lead to the breakdown of the academic enterprise, and therefore serious consequences arise and harsh sanctions are imposed. For example, incidences of plagiarism or cheating may result in a mark of zero on the assignment or exam and more serious consequences may apply when the matter is referred to the Office of the Dean. Careful records are kept in order to monitor and prevent recurrences. A more detailed description of academic integrity, including the University's policies and procedures, may be found in the UBC Calendar: Student Conduct and Discipline.

Academic Accommodation for Students with Disabilities: Academic accommodations help students with a disability or ongoing medical condition overcome challenges that may affect their academic success. Students requiring academic accommodations must register with the Centre for Accessibility (previously known as Access & Diversity). The Centre will determine that student's eligibility for accommodations in accordance with Policy 73: Academic Accommodation for Students with Disabilities. Academic accommodations are not determined by your instructors, and instructors should not ask you about the nature of your disability or ongoing medical condition, or request copies of your disability documentation. However, your instructor may consult with the Centre for Accessibility should the accommodations affect the essential learning outcomes of a course.

Conflicting Responsibilities: UBC recognizes that students may occasionally have conflicting responsibilities that affect their ability to attend class or examinations. These may include: representing the University, the province or the country in a competition or performance; serving in the Canadian military; or observing a religious rite. They may also include a change in a student's situation that unexpectedly requires that student to work or take responsibility for the care of a family member, if these were not pre-existing situations at the start of term.

Students with conflicting responsibilities have a duty to arrange their course schedules so as to avoid, as much as possible, any conflicts with course requirements. As soon as conflicting responsibilities arise, students must notify either their instructor(s) or their Faculty Advising Office (e.g. Arts Academic Advising), and can request academic concession. Instructors may not be able to comply with all such requests if the academic standards and integrity of the course or program would be compromised.

Varsity student-athletes should discuss any anticipated and unavoidable regular-season absences with the instructor at the start of term, and provide notice of playoff or championship absences in writing as soon as dates are confirmed.

Religious observance may preclude attending classes or examinations at certain times. In accordance with the UBC Policy on Religious Holidays, students who wish to be accommodated for religious reasons must notify their instructors in writing at least two weeks in advance. Instructors provide opportunity for such students to make up work or examinations missed without penalty.