

COURSE INFORMATION

- COMM 338 is offered for students interested in learning the fundamentals of cybersecurity
- Learning activities: lectures, team project, case analysis, hands-on labs, in-class exercises, quiz
- Participation is important for your learning; we will use iClickers and work in teams
- Course Syllabus (this) may be updated periodically so check Canvas regularly
- Assignment and lab briefs will be posted to Canvas
- No textbook required; use pre-lecture materials and module slides to prep for assignments/quiz
- Recommended to read the course syllabus in full; ask ahead of time if things are unclear

Course title:	Management of Cybersecurity		
Course code:	COMM 338	Credits:	3
Session and term:	2025/26 W1	Class location:	HA 295
Section(s):	101	Class times:	Mon 5-8 pm (regular) First class only: Thurs Sep 4 from 7-10pm in HA347
Course duration:	2025-09-02 - 2025-12-01	Pre-requisites:	See course webpage.
Division:	AIS	Co-requisites:	n/a

INSTRUCTOR INFORMATION

Instructor:	Liam Adams, CISSP	Office location:	Virtual or HA 349
Phone:	email me instead	Office hours:	By appointment
Email:	liam.adams@sauder.ubc.ca		
TA:	Filip Herle Hamza Ahmad		

COURSE DESCRIPTION & FORMAT

As many organizations increasingly transform to adopt digital business models with the use of emerging technologies, the need for these organizations to develop comprehensive cybersecurity programs has become apparent. Cybersecurity has been recognized as one of the preeminent challenges of our time. Business and IT professionals need to understand the fundamentals of cybersecurity in order to effectively communicate about cyber risk within their organizations.

Designed to be accessible for students from a variety of educational backgrounds (technical or non-technical), this in-person course will introduce you to the principles that frame and define cybersecurity, and the role of cybersecurity practitioners, processes and technology in the protection of enterprise assets from external and insider threats. You will also have the opportunity to apply concepts during guided hands-on labs while being exposed to industry tools and frameworks.



LEARNING OBJECTIVES

By the end of this course, students should be able to:

1. Design and manage an organization's cybersecurity strategy and architecture.
2. Communicate effectively about cybersecurity issues with business and technology teams.
3. Gain hands-on experience with cybersecurity tools, technologies and key concepts.
4. Discuss strategies to manage security threats, vulnerabilities, and risks.
5. Describe different threat actors, their motivations and common attack vectors.

SUSTAINABLE DEVELOPMENT GOALS (SDGS)

At UBC Sauder, we are committed to responsible business practices that can have transformative impacts on society. One of the ways we are reinforcing our commitment to responsible business is by showcasing relevant content in our courses via the lens of the [United Nations Sustainable Development Goals](#). In this course, we will touch on topics that relate to the following goals:

Sustainable Development Goal	Description of how and when the goal is covered in the course.
Goal 5: Gender Equality 	In week 1 through the course introduction and security governance lectures we will talk about the importance of promoting women in the cybersecurity field and opportunities for women to network with other women already in the field (e.g. PwC's SheProtects)
Goal 9: Industry, Innovation and Infrastructure 	In weeks 4 and 5, we will talk about the role of cybersecurity practitioners in the protection of critical infrastructure and ensuring the availability and resiliency of critical services. We will also study a case that will illuminate the danger of cyber threats to critical infrastructure and supply chains.

ASSESSMENTS

Component		<u>Weight</u>
Cases (x3)	Team-based	30%
Labs (x4)	Pairs or individual	10%
Team Project	Team-based	30%
Quiz (x2)	Individual	15%
Reflection	Individual	5%
Participation	Individual	<u>10%</u>
Total		<u>100%</u>

Details of Assessments and Learning Activities

Activity	Description	Tips for success
Pre-lecture preparation	Pre-lecture materials help you prepare for class. There is no assigned textbook for this course.	<ul style="list-style-type: none"> Plan enough time to review and reflect on materials before class; note down questions
Lecture modules + In-class Exercises (ICE)	During lectures we will introduce course concepts through real-life examples, and engage collectively in active discussion. Lecture module slides will act as the course textbook and can be used to prepare for Quizzes. Some modules will also have in-class exercises where you can apply concepts.	<ul style="list-style-type: none"> Ask questions Offer your opinions Present your ideas Share your experiences Use a name card initially
Case Analyses	You will work in teams to write a case deliverable that analyzes and discusses key issues of the case. Each case will be debriefed post-submission during the class date on which the case deliverable is due.	<ul style="list-style-type: none"> Understand the grading rubric Read the case at least twice and markup your notes Have someone proofread your deliverable to catch spelling/grammar errors, ensure flow and consistent writing style, etc. Tell a story through your analysis; remember your audience
Guest speakers	On special occasions during the semester, an industry professional with experience in the cybersecurity field may be invited to speak. You'll have the opportunity to engage and network with them to better understand their day-to-day work.	<ul style="list-style-type: none"> Ask questions Offer your opinions Present your ideas Share your experiences Use a name card Read about the topic in advance to form a view
Labs	Labs will offer you the opportunity to apply course concepts in a practical and hands-on manner using real-world security tools. No prior experience is required. You will complete the lab during class time either on your own or with a peer. You will submit a lab deliverable describing your solution/answers to the lab problem.	<ul style="list-style-type: none"> Work with a classmate to complete the lab so that you can bounce ideas off of each other if you get stuck Don't rush through the lab; focus on building your skills
Quiz	We will have short quizzes (~20 MCQs) during the term. Quizzes will contain mostly multiple choice questions aimed at assessing your understanding of topics covered during lectures. Use the lecture slides to prepare.	<ul style="list-style-type: none"> Budget enough time to review past lecture content Review past iClicker questions Come up with your own questions and quiz your peers
Participation	Participation will be a part of your final grade	<ul style="list-style-type: none"> Ask questions Provide your opinions

	<p>because of how important participation is in the real-world. In your future roles you will likely need to clearly articulate, communicate, and present your ideas to stakeholders. Your participation grade will be determined based on the frequency and quality of your class participation. You will have many chances to participate over the course of the term.</p>	<ul style="list-style-type: none"> ● Present your ideas ● Share your experiences ● Get to know your classmates; listen to their questions, ideas and experiences
Team Project	<p>The team project is an opportunity for you to apply course concepts while working with your peers to research a real-world cybersecurity incident or problem, of your choice, which has impacted an organization. Your project proposal will be validated by a member of the teaching team.</p> <p>Optional: For teams who want to flex their technical skills, you can think about ways to be creative in demonstrating the incident, issue or problem affecting your chosen entity in a safe way (e.g., setting up a lab environment to demo how a vulnerability was exploited).</p>	<ul style="list-style-type: none"> ● Understand the grading rubric ● Choose a research topic with enough publicly available information ● Have someone proofread your deliverable to catch spelling/grammar errors, ensure flow and consistent writing style, etc. ● Consider each of your team members' strengths and play to them ● Don't let your team carry you; contribute fairly
Reflection	<p>The reflection assignment enables you to introspectively think about the course content and what you have learned this semester. It's a nice motivator to document your key takeaways as you progress through the course.</p>	<ul style="list-style-type: none"> ● Reflect after each lecture and note down your thoughts in a notebook (virtual or physical) ● Note down any expectations you have for your learning, the course, etc., on day 1 and compare later on

LEARNING MATERIALS

Required: No textbook. Course Package can be purchased following the instructions below.

Estimated cost of required materials is < \$20

Additional materials required: See Canvas and course schedule for readings/videos etc.

Go to the Ivey Publishing website at www.iveypublishing.ca

1. Log in to your existing account or click "Register" to create a new account and follow the prompts to complete the registration. If registering, choose the "Student" role.
2. Click on this link or copy into your browser:
<https://www.iveypublishing.ca/s/ivey-coursepack/a1ROF000004uODR2A2>
3. Click "Add to Cart".
4. Go to the Shopping Cart (located at the top of the page), click "Checkout", and complete the checkout process
5. When payment has been processed successfully, from the Order Confirmation screen, click on "Access Purchases", then click "Downloads". Note: Access to downloadable files will expire on the course end date, so be sure to save a copy on your computer.

NO DISTRIBUTION OF RECORDINGS

There is no distribution of recordings of class. Classes are designed as and are intended to be in-person. Your attendance is expected. If you are unable to attend, the policy regarding missed classes described in this syllabus applies. It is your responsibility to ensure that you have the materials you need for missed classes. It is strongly recommended that you make arrangements at the start of the semester for materials in case you miss class. For instance, you may wish to exchange contact information with a classmate who can provide you with notes in the event you miss class. If you believe you are an exceptional case that merits special consideration, please promptly reach out to your instructor to advise them of your circumstances.

ACADEMIC CONCESSIONS

Academic Concession Policy

Only the Sauder Office of Student Academic Services ("OSAS") can approve an absence from class, so all documentation for absences/illness should be submitted to the OSAS (email: osasoperations@sauder.ubc.ca), not to your instructor. Job interviews, club meetings, networking events or other extracurricular activities are not acceptable reasons to miss class. If you miss a single class due to illness, let your instructor know. If you miss multiple classes, let the OSAS know.

No penalty will be assessed for a missed assignment if the OSAS grants you an academic concession, but you must still turn in your assignment after a reasonable period of time. If you do not contribute sufficiently to any team-based assignments, you may be asked to leave the team and could receive a grade of zero.

Requesting Academic Concession

If you experience unanticipated events or other circumstances that constitute valid grounds for academic concession as defined by [UBC's Academic Concession Policy](#), complete the [concession request webform](#). Concessions are time-sensitive and the webform should be submitted within 48 hours of the missed deadline. Upon submission, your request will be recorded in the OSAS and you will also receive an email with further instructions. Please read this email carefully and be sure to also refer to the relevant course syllabus for each concession that you have requested. Please know that you should continue to work on

the coursework for the course(s) which you submitted a concession for. You should anticipate being asked to submit work or write an exam as soon as the circumstances affecting your ability to fulfill your academic responsibilities are resolved.

COURSE-SPECIFIC POLICIES AND RESOURCES

Use of GenAI

Generative Artificial Intelligence (GenAI) technologies are widely available and are increasingly intertwined with teaching and learning. The term “GenAI” refers to the following tools as well as any other similar models that create content using sophisticated learning algorithms: ChatGPT, Claude, Copilot, Gemini, Llama, DeepSeek, and many translation tools. GenAI also refers to such tools that may be integrated into other services like Notion, Canva, and Grammarly.

Sauder considers it essential that 1) students develop proficiency with GenAI; and 2) students are able to learn and practice the foundational critical thinking skills, unaided by GenAI, that are essential to a university education. To achieve both of these goals requires a mix of assessments that use GenAI and those that do not. Therefore each assessment will include GenAI instructions that are best suited to its learning objectives and that uphold Sauder’s commitment to academic integrity. Your instructor will specify, for each assessment, which one of the following usage rules is in effect.

- A. GenAI is Permitted, with attribution. Your instructor will explain what form of attribution, or what citation format, is required. Your instructor may also explain how GenAI may be used if/when it isn’t fully permitted.
- B. GenAI is Prohibited, in a controlled environment. Your instructor will provide a controlled environment for the assessment, such as an exam using lockdown browser or a pen and paper classroom activity.
- C. GenAI is Required, as part of the assessment. Your instructor will provide instructions describing how GenAI is expected to be used (including instructions regarding attribution/citation, if applicable).
- D. GenAI is Discouraged, for a low-stakes formative assessment. Students are expected to work on the assessment without GenAI assistance, e.g., in order to practice or increase knowledge/skills on course content.

After review, if it is determined by the instructor that submitted work likely violates the Use of GenAI policy and/or the specific usage rule, the work may receive a zero and may be subject to further misconduct measures set out in the UBC Academic Calendar.

GenAI and groups/teams: Group work is an important part of this course, however, it introduces additional challenges around GenAI use. Therefore, whenever GenAI is permitted for a group assessment, the group must hold a discussion, with all members present, when beginning the work. During this discussion the group must agree on whether, how, and by whom GenAI tools will be used (to be documented in a shared file or email). All group members are expected to then communicate honestly with their group about their own use of GenAI. If it is determined that GenAI was used in a way that violates the assessment’s rules, the entire group may be held responsible.

Missed or late assignments, and regrading of assessments

It is your responsibility to plan your time carefully. If you miss an assignment deadline, you will receive a grade of zero for that assignment unless the circumstances warrant a different outcome.

Assignment formatting requirements

Assignments should be submitted as PDF documents and follow the following formatting requirements, unless stated differently in the assignment brief document:

- Font: Arial
- Font size: minimum 10 point
- Margins, headers and footers: 1" (2.54cm)
- Pages: one-inch margins and numbered from page two
- Page numbers at bottom right corner
- Single line spacing
- All text should be left-aligned
- Include a title page with your name, team name, team member names, submission date

ACADEMIC ACCOMMODATIONS

Centre for Accessibility

The [Centre for Accessibility](#) (CfA) facilitates disability-related accommodations and programming initiatives designed to remove barriers for students with disabilities and ongoing medical conditions. If you are registered with the CfA and are eligible for exam accommodations, it is your responsibility to book your exam writing with the CfA using its [exam reservation system](#): for midterm exams or quizzes, at least 7 days in advance; and final exams, 7 days before the start of the formal exam period.

POLICIES APPLICABLE TO UBC SAUDER UNDERGRADUATE COURSES

At UBC Sauder, professional behaviour aligns with the school's guiding values – rigour, respect and responsibility – and is upheld in the [UBC Sauder BCom Statement of Professionalism and Code of Conduct](#).

Respectfulness in the classroom

Students are expected to be respectful of our community at all times, including community members, faculty, staff and peers. This means being attentive and conscious of words and actions and their impact on others, listening to people with an open mind, treating all UBC Sauder community members equally and understanding diversity. Students who act disrespectfully toward others will be asked to leave the class and be marked as absent for the day. They may also be removed from a team, lose credit for in-class assessments and activities, or be asked to complete a group assignment individually. Incidents of misconduct or suspected misconduct will be investigated.

Respect for Equity, Diversity, and Inclusion

The UBC Sauder School of Business strives to promote an intellectual community that is enhanced by diversity along various dimensions including Indigeneity (including identification as First Nation, Métis, or Inuit), race, ethnicity, gender identity, sexual orientation, religion, political beliefs, social class, and/or disability. It is critical that students from diverse backgrounds and perspectives be valued in and well-served by their courses. Furthermore, the diversity that students bring to the classroom should be viewed as a resource, benefit, and source of strength for your learning experience. It is expected that all students and members of our community conduct themselves with empathy and respect for others.

UNIVERSITY POLICIES AND RESOURCES

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 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 on the UBC Senate website at

<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 university policies and codes of conduct regarding academic integrity. At the most basic level, this means consistently 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; nor should you help others to do the same. For example, it is prohibited to: share your past assignments and answers with other students; work with other students on an assignment when an instructor has not expressly given permission; or spread information through word of mouth, social media, or other channels that subverts the fair evaluation of a class exercise, or assessment. 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 if the matter is referred to the President's Advisory Committee on Student Discipline. Careful records are kept in order to monitor and prevent recurrences.

COPYRIGHT

All materials of this course (course handouts, lecture slides, assessments, course readings, etc.) are the intellectual property of the instructor or licensed to be used in this course by the copyright owner. Redistribution of these materials by any means without permission of the copyright holder(s) constitutes a breach of copyright and may lead to academic discipline and could be subject to legal action. Any lecture recordings are for the sole use of the instructor and students enrolled in the class. In no case may the lecture recording or part of the recording be used by students for any other purpose, either personal or commercial. Further, audio or video recording of classes are not permitted without the prior consent of the instructor.

ACKNOWLEDGEMENT

UBC's Point Grey Campus is located on the traditional, ancestral, and unceded territory of the x̱məθḵw̱əy̱əm (Musqueam) people, who for millennia have passed on their culture, history, and traditions from one generation to the next on this site.

THIRD PARTY VENDOR TOOLS

In this course, students will be using cloud-based tools and software provided by third-party vendors (including Axio360, Cisco/Duo Security, Splunk, Kali Linux, Microsoft Azure, among others). These tools

will help us perform the lab component of the course. During the account creation process, you may be required to provide your name, email and other identifying information. By using these services, you are consenting to storage of your information in the location where the service is hosted. If you choose not to provide your consent, see the instructor for alternate arrangements. You may also consider providing an alias as a way of protecting your identity.

COURSE SCHEDULE

All pre-class prep materials (readings, videos, podcasts, etc.) should be reviewed and/or completed prior to the date of each class.

Remember the class schedule below may change with advance class notification.

Monday	Tuesday	Wed.	Thursday	Friday
<p><i>Sep 1</i></p> <p><i>No class</i></p>	<p><i>Sep 2</i></p> <p><i>Imagine Day</i></p>	<p><i>Sep 3</i></p>	<p><i>Sep 4</i></p> <p>Module 0: Course Welcome & Intros</p> <p>Reading: (this) Course Outline</p> <p>Video: Course teaser (link)</p> <p>//</p> <p>Module 1: Security Governance</p> <p>Reading: What is a Security Policy? (link)</p> <p>ICE: Team formation</p>	<p><i>Sep 5</i></p>

<p>Sep 8</p> <p>Class rescheduled to Sep 4th</p>	Sep 9	Sep 10	Sep 11	Sep 12
<p>Sep 15</p> <p>Module 2: Risk Management Strategy</p> <p>Reading: The Relationship Between Business Risk and Security and the Role of the Modern CISO, Exabeam (link)</p> <p>Reading: Eight Steps to Manage the Third-Party Lifecycle, ISACA blog (link)</p> <p>ICE: Risk appetite statements</p> <p>//</p> <p>Module 3: Security Threat Risk Assessments</p> <p>Reading: Introducing STRAs (link) (read up to the end of the “When to Consider an STRA?” section)</p> <p>ICE: Axio360</p>	Sep 16	Sep 17	<p>Sep 18</p> <p>Due: Team charter (see Team Project assignment brief posted to Canvas).</p>	Sep 19
<p>Sep 22</p> <p>Module 4: Organizational Resilience & Disaster Recovery</p> <p>Reading: DR Strategy: Types of Alternate Sites (link)</p> <p>Reading: Protecting the Crown Jewels, Information Security Forum (download from Canvas)</p> <p>ICE: Recovery objectives for crown jewels</p>	Sep 23	Sep 24	Sep 25	Sep 26

<p>//</p> <p>Case Debrief: Cyberattack: The Maersk Global Supply-Chain Meltdown</p> <p>Due: Assignment #1</p> <p>Assignment brief will be posted on Canvas</p>				
<p>Sep 29</p> <p>Module 5: Cryptography Basics</p> <p>Video: Public Key Cryptography: What is it?, Khan Academy (link)</p> <p>Reading: "Schneier's Law" - ignore the comments section (link)</p> <p>ICE: Exploring PGP encryption tool</p> <p>Due: Project proposal</p> <p>//</p> <p>Lab #1: Cisco + Duo Security Identity Intelligence</p> <p>Guest: Scott Henry, Data Science, Technical Lead at Cisco / Duo Security</p> <p>Pre-lab will be posted to Canvas.</p>	<p>Sep 30</p> <p>National Day for Truth and Recon.</p>	<p>Oct 1</p>	<p>Oct 2</p>	<p>Oct 3</p>
<p>Oct 6</p> <p>Module 6: Security Threats & Attack Vectors</p> <p>Reading: Computer Networking Basics - posted under Resources on Canvas</p> <p>Video: Google's Charles Carmakal explores top threats to public sector (link)</p> <p>Optional Reading: Written Testimony</p>	<p>Oct 7</p>	<p>Oct 8</p>	<p>Oct 9</p>	<p>Oct 10</p>

<p>from Charles Carmakal on Countering the Cyberthreat from China (link). Note you can disregard the section “Difficulty in Discovering Compromises” for now</p> <p>ICE: Packet sniffing with Wireshark</p> <p>//</p> <p>Case Debrief: Data Breach at Equifax</p> <p>Due: Assignment #2</p> <p>Assignment brief will be posted on Canvas</p> <p>Guest: TBD.</p>				
<p>Oct 13</p> <p>Thanksgiving Day</p> <p>No class</p>	Oct 14	Oct 15	Oct 16	Oct 17
<p>Oct 20</p> <p>Module 7: Identity & Access Management</p> <p>Reading: Privileged Access Management, CyberArk (link)</p> <p>Reading: The Ongoing Fallout from a Breach at AI Chatbot Maker Salesloft (link)</p> <p>ICE: Delegated access problem</p> <p>//</p> <p>Lab #2: Microsoft Entra ID (Azure Active Directory)</p> <p>Pre-lab will be posted on Canvas</p>	Oct 21	Oct 22	Oct 23	Oct 24

<p>Oct 27</p> <p>Module 8: Security Architecture & Design</p> <p>Video: Security Controls - Types, Categories, and Functions (link)</p> <p>Reading: Define Security Requirements, OWASP Top Ten Proactive Controls 2018 (link)</p> <p>Reading: Address Security from the Start, OWASP Top Ten Proactive Controls 2024 (link)</p> <p>ICE: Creating threat models</p> <p>//</p> <p>Case Debrief: Ransomware Attack at Colonial Pipeline Company</p> <p>Due: Assignment #3</p> <p>Assignment brief will be posted on Canvas</p> <p>Guest: TBD.</p>	Oct 28	Oct 29	Oct 30	Oct 31
<p>Nov 3</p> <p>Module 8: DevSecOps</p> <p>Reading: What is DevSecOps, Red Hat (link)</p> <p>Reading: How to start an AppSec Program (link)</p> <p>Quiz 1 [Topics covered to date]</p> <p>Demo: Security in software pipelines</p> <p>//</p> <p>Simulation: Game of Threats - get ready to play as attackers and defenders!</p>	Nov 4	Nov 5	Nov 6	Nov 7

<p>Optional: Bring a friend who may want to take the course next term!</p>				
<p>Nov 10</p> <p>Midterm break</p>	<p>Nov 11</p> <p>Remembrance Day (observed)</p>	<p>Nov 12</p> <p>Midterm break</p>	<p>Nov 13</p>	<p>Nov 14</p>
<p>Nov 17</p> <p>Module 9: Managing Security Operations</p> <p>Reading: Vulnerability Management Process, Rapid7 (link)</p> <p>Reading: Siemens and Rockwell Tackle Industrial Cybersecurity, but Face Customer Hesitation, SecurityWeek (link)</p> <p>Podcast: Using Red Teaming to Improve Your Security (link)</p> <p>ICE: Port scanning with nmap</p> <p>//</p> <p>Lab #3: Offensive Security with Kali Linux</p> <p>Pre-lab will be posted on Canvas</p>	<p>Nov 18</p>	<p>Nov 19</p>	<p>Nov 20</p>	<p>Nov 21</p>
<p>Nov 24</p> <p>Module 10: Incident Detection & Response</p> <p>Video: Inside the Security Operations Centre, Akamai (link)</p> <p>Video: What is the Common Security Advisory Framework?, CSAF (link)</p>	<p>Nov 25</p>	<p>Nov 26</p>	<p>Nov 27</p>	<p>Nov 28</p>

<p>Reading: What is EDR?, Cisco (link)</p> <p>Quiz 2 [Topics covered to date]</p> <p>ICE: ATT&CK use case mapping</p> <p>//</p> <p>Lab #4: Splunk for security investigations</p> <p>Pre-lab will be posted on Canvas</p>				
<p>Dec 1</p> <p>In-class Presentations</p> <p>Order for presentations will be randomly decided.</p> <p>Due: <u>All</u> Team project presentation decks</p>	Dec 2	Dec 3	<p>Dec 4</p> <p>Potential Extra Class, if required—TBD</p> <p>Due: Team project analysis report</p>	<p>Dec 5</p> <p>Last day of classes</p> <p>Due: Reflection</p>
Dec 8	Dec 9	Dec 10	Dec 11	Dec 12
Dec 15	Dec 16	Dec 17	Dec 18	Dec 19