Cyber Security – Post Graduate Certificate

PLAR Candidate Guide

Prior Learning Assessment and Recognition (PLAR)

Copyright

Prior learning credit options at Saskatchewan Polytechnic

See Get Credit for What you Know for important information about all options to get credit for prior learning at Sask Polytech, including PLAR, transfer credit, Canadian Armed Forces credit, and equivalency credit.

How to navigate this document

This document contains links to other document sections or webpages. To return to where you were from another section in this document, press the *ALT* key and *left arrow* key at the same time. To return to this webpage from another webpage, close the other webpage or click back on the browser tab for this document.

Contents of this guide

This guide contains the following specific PLAR information and tools for this program

A. PLAR fees

Fees for PLAR challenges are set to cover our costs for consultation, assessment, and related administrative tasks. PLAR fees are non-refundable and non-transferrable.

The PLAR fees policy is subject to change for each new academic year. Please see the **Cost** section on the PLAR webpage for current fee information.

B. PLAR eligibility and options

To be eligible for PLAR you must be a student registered at Sask Polytech. You must also consult with the PLAR contact person and be approved for PLAR assessment.

Course pre-requisites and co-requisites

Some courses have one or more other courses that must be completed first (pre-requisite) or at the same time (co-requisite). See course outlines in this guide to identify any pre- or co-requisites for each course. Discuss with your PLAR contact person how to deal with courses with co-requisites.

Block assessment

Some programs may assess a cluster of courses together in one block, which may save you time and effort. Ask the PLAR contact person whether there are any block assessment options in this program.

C. Dates when PLAR assessment is available

PLAR assessment for this program is available from Sept 1 to June 15 in each academic year.

All PLAR assessment must be completed by June 15 of each academic year.

D. Special directions for this program

1. **Review** the PLAR process and FAQs and the information in this guide.

2. **Self-rate** your learning for each course using the Course Outlines in this guide.

3. **Consult** with the PLAR contact person for PLAR approval. Be prepared to provide your resume, course self-ratings (see section F), and a partially completed PLAR application. If you are approved for PLAR, the contact person will sign your PLAR application and explain next steps.

4. **Register** for PLAR at Registration Services once you have signed approval on your PLAR Application Form. The PLAR fee will be added to your student account.

5. **Complete** assessment before your PLAR registration expires.

E. PLAR contact person

Contact the person below to arrange a consultation **after** you have read this guide and general PLAR information **and** rated yourself for each course (see next session). Consultation may be by phone, online, or in person. Be prepared to provide your resume, course self-ratings, and a partially completed PLAR application. If agreement is reached to go ahead with PLAR, the contact person will sign approval on your PLAR application and explain the next steps. Admission to the program is required before you can register for PLAR.

Mayra Samaniego, Program Head
Cyber Security Post Graduate Certificate
Saskatchewan Polytechnic, Saskatoon Campus
PH: 306 – 659 - 4591
Email: mayra.samaniego@saskpolytech.ca

F. Self-rating course outlines

Clicking on a course code below opens a page where you can rate yourself on the knowledge and skills assessed for PLAR credit. For Arts & Sciences courses, clicking on the course code opens another PLAR guide. The PLAR contact person for this program will refer you to another person to discuss PLAR for courses delivered by Arts & Sciences or another program/department.

COURSE CODE	COURSE NAME	Delivered by another department/program
	Semester 1	
CNET 601	Routing and Switching	
CSEC 600	Operating Systems and Applications Security	
CSEC 601	Web Security	
CSEC 602	Security Planning	
TCOM 600	Business Technology Communications	Arts & Sciences
	Semester 2	
CSEC 603	Information Security Testing	
CSEC 605	Network Monitoring and Penetration Testing	
CSEC 606	Ethical Hacking and Exploits	
CSEC 608	Cloud Security	
INDG 600	Indigenous Studies	Arts & Sciences
INTL 600	Information Technology	
	Semester 3	

COURSE CODE	COURSE NAME	Delivered by another department/program
CSEC 607	Digital Forensics	
INTL 601	Information Technology Auditing	
PROJ 603	Capstone Project	

CNET 601 – Routing and Switching

You will describe the roles of routers and switches in an enterprise network and analyze their operation. Your studies will include switching; Spanning Tree Protocol (STP); Virtual Local Area Networks (VLANs); routing protocols, Internet Address Protocols, IPv4 & IPv6; inter-VLAN routing; Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). The course content is based on the Cisco Certified Network Associate (CCNA) Routing & Switching Essentials curriculum.

Credit unit(s): 3.0
Pre and Co Requisites: none
Equivalent course(s): none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Examine the methods routers and switches use to make packet forwarding decisions including Virtual Local Area Networks (VLANs) and trunking with tags.			
2. Examine the addressing format of the IPv4 and IPv6 protocols and perform calculations to implement an addressing scheme that utilize multiple subnetworks.			
3. Analyze the structure of an Internet Protocol (IP) routing table to determine how the elements are used to forward packets.			
4. Configure static and default routes for inclusion in the route table and compare them to the dynamic routing protocols.			
5. Troubleshoot IP networks that implement VLANs, VLAN trunking with 802.1Q, static routes and routing with RIP.			
6. Configure standard and extended access control lists on Cisco routers and examine their functions to control network traffic.			
7. Configure DHCP and NAT.			
8. Configure a network and device management on a network.			

CSEC 600 – Operating Systems and Applications Security

You will focus on the vulnerabilities of Windows and Linux operating systems. Your studies will include the best practices and methodologies to ensure that critical security upgrades and system patches are installed. You will explore vulnerabilities to web applications.

Credit unit(s):	3.0
Pre and Co Requisites:	none
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Discuss the concepts of vulnerability testing and the use of vulnerability scanning tools.			
2. Explain how Metasploit is used for penetration testing.			
3. Discuss wireless vulnerabilities in networks.			
4. Differentiate between host Intrusion Detection Systems (IDS) and network IDS.			
5. Explain the importance of login security.			
6. Assess the recommendations provided to clients following the execution of risk analysis and/or the implementation of risk management strategy.			

CSEC 601 - Web Security

You will delve into the current scripting and computer languages used by modern web clients and servers. Your focus will be on the programming methodologies used to prevent exploitation of web security vulnerabilities.

Credit unit(s):	3.0
Pre and Co Requisites:	none
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Describe the basic syntax and use of Hypertext Markup Language (HTML) and Cascading Style Sheets (CSS).			
2. Explain the basic features and syntax of JavaScript.			
3. Describe the security issues surrounding client-side scripting and how to address the security issues.			
4. Develop a website to include active content.			
5. Describe the basic features and syntax of Hypertext Preprocessor (PHP).			
6. Describe the concept of session management and how cookies facilitate this form of server communication.			
7. Explain the methods used to protect session cookies.			
8. Describe how databases are used by websites to store client information.			
9. Develop a backend architecture using PHP and a database to serve a website.			

CSEC 602 – Security Planning

You will develop the skills to identify essential elements of a Security Management System and the business processes that require protection. You will develop the skills and knowledge to conduct risk assessments that will identify vulnerabilities and countermeasures to prevent and mitigate system failures. You will be able to identify the consequences of data loss and the safeguards to prevent data loss. Your studies will concentrate on the principles of implementing security in an organization, the preparation of cybersecurity policies and the assessment of effectiveness of existing cybersecurity policies.

Credit unit(s):	3.0
Pre and Co Requisites:	none
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Explain the principles of information security and the impact of organizational attributes on information security.			
2. Describe the attributes of a security management system and implementations strategies.			
3. Differentiate among security policy, standards, guidelines and procedures.			
4. Create specimen security policies for an organization.			
5. Describe risk assessment.			
6. Identify the vulnerabilities and threats to the business/information processes due to natural events, human error and infrastructure failures or malicious activities.			
7. Describe the issues in implementing the principles of security awareness and user education.			
8. Explain an organization’s responsibility for the ethical protection of organizational and personal information.			
9. Discuss the financial legal and regulatory issues affecting information security and their impact on the enterprise.			

TCOM 600 – Business Technology Communications

You will learn how to manage communication in a business environment using best practices and common software tools. You will learn how to produce effective content delivered with appropriate tools.

Credit unit(s): 3.0
Pre and Co Requisites: none
Equivalent course(s): none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Write effective communication from template documents.			
2. Create long form documents using word processing software.			
3. Produce a workflow diagram in Visio.			
4. Create effective reports and dashboards with Excel.			
5. Integrate communication tools into an effective presentation.			
6. Prepare a Request for Proposal document using a standard process.			

CSEC 603 – Information Security Testing

You will learn how cyber-attacks penetrate Information Technology (IT) systems by circumventing security or exploiting vulnerabilities in the systems. You will apply a methodical approach to surveying, testing and auditing systems, and you will learn to prepare secure system designs, identify vulnerabilities, and defend systems against intrusion.

Credit unit(s):	3.0
Pre and Co Requisites:	CSEC 602
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Describe the legal and contractual aspects involved in security and penetration testing.			
2. Explain the ethical position concerning security testing versus hacking.			
3. Discuss the common approaches and methodologies used for carrying out and managing security and penetration testing.			
4. Describe network protocols and relevant computer system architectures.			
5. Identify vulnerabilities in existing protocols, systems and applications, and common forms of attack.			
6. Demonstrate how these vulnerabilities may be exploited to penetrate a system.			
7. Discuss the pros and cons of the black/white box testing.			
8. Deploy configured Virtual Machines (VMs) for the purpose of conducting security testing.			
9. Discuss the importance of communicating to all audiences (technical and non-technical) of business about the need for ongoing Information Systems Management (ISM) testing.			

CSEC 605 – Network Monitoring and Penetration Testing

You will learn techniques used to monitor networks for unauthorized access. Your studies will include the concept of ethical hacking and the tools and methods systems used to test the security of systems currently in operation.

Credit unit(s):	3.0
Pre and Co Requisites:	CSEC 600, INTL 600, CNET 601
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Discuss the ethics for security ethical hacking and penetration testing.			
2. Explain the steps in the hacker methodology.			
3. Discuss the concepts of vulnerability testing and the use of vulnerability scanning tools.			
4. Determine how metasploit is used for penetration testing.			
5. Determine wireless vulnerabilities in networks.			
6. Differentiate between host Intrusion Detection System (IDS) and network IDS.			
7. Determine importance of login security.			
8. Assess the recommendations provided to clients following the execution of risk analysis and/or the implementation of risk management strategy.			

CSEC 606 – Ethical Hacking and Exploits

You will learn various attack and defense methodologies. While exploring current and emerging security topics you will learn how computer security affects businesses and business data. You will be introduced to the protection of an organization's assets, intellectual property and employees as well as methods for maintaining business continuity.

Credit unit(s):	3.0
Pre and Co Requisites:	CSEC 602
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Evaluate ethical hacking.			
2. Apply the techniques of information gathering.			
3. Analyze attack and defense methodologies.			
4. Demonstrate mobile and wireless security.			
5. Demonstrate internet of things security.			
6. Discuss cloud security.			
7. Investigate social engineering.			
8. Examine cyber warfare and advanced topics.			

CSEC 608 – Cloud Security

You will delve into the use of cloud computing services. You will be able to identify the benefits and downsides of integrating cloud-based services in a company's operation. You will study best practices to manage the configuration and security of cloud environments to host business applications. You will develop the skills and knowledge to conduct evaluations of cloud adoption and migration.

Credit unit(s): 3.0
Pre and Co Requisites: CNET 601, CSEC 600, INTL 600
Equivalent course(s): none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Explain the principles and features of cloud computing.			
2. Differentiate among infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).			
3. Revise security concerns when using software as a service (SaaS).			
4. Evaluate how to secure platform as a service (PaaS) environments for the deployment of applications.			
5. Evaluate networking security in infrastructure as a service (IaaS) business scenarios.			
6. Explain cloud storage.			
7. Describe cloud data security.			
8. Evaluate cloud computing threats and vulnerabilities.			
9. Analyze cloud-computing adoption and migration for different scenarios.			

INDG 600 – Indigenous Studies

You will complete the Blanket Exercise to honour the Indigenous peoples in Canada. You will study the history of the relationships between European settlers and the Indigenous peoples from initial contact to present day. You will analyze the 94 Calls to Action of the Truth and Reconciliation Commission to redress the legacy of residential schools and advance Canadian reconciliation.

Credit unit(s):	1.0
Pre and Co Requisites:	none
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Complete the Blanket Exercise to honour Indigenous peoples in Canada.			
2. Examine the history of relationships between European Settlers and Indigenous peoples.			
3. Analyze the Truth and Reconciliation Commission of Canada and the 94 Calls to Action.			

INTL 600 – Information Technology

You will learn the essential concepts of information security triad, confidentiality, integrity, and availability (CIA). You will examine the common vulnerabilities in computer and network systems and the methodology hackers use to exploit these systems.

Credit unit(s):	3.0
Pre and Co Requisites:	none
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Describe the actions of social engineering tools and malware such as viruses, worms and remote access Trojan programs.			
2. Evaluate the different encryption algorithms such as symmetric and asymmetric used to protect and secure user data.			
3. Examine public key encryption.			
4. Create secure authentication.			
5. Explain the difference between the secure socket layer/transport layer secure (SSL/TLS) and secure shell (SSH) protocols for secure communications.			
6. Analyze the methods used by hackers to attack computer networks.			
7. Compare the actions taken by the different types of transmission control protocol/internet protocol (TCP/IP) based network attacks.			
8. Evaluate the processes used in the remote authentication dial-in user service (RADIUS) and Kerberos protocols to implement authentication, authorization and accounting services to provide access control.			
9. Describe the operation of wireless networks and how the IEEE802.11i media access control protocol addresses security issues for authentication and data confidentiality.			

CSEC 607 – Digital Forensics

You will study the principals of digital forensics to detect, recover, trace, analyze and interpret digital evidence. You will file structure, data recovery techniques, data hiding and the process for conducting a digital investigation.

Credit unit(s): 3.0
Pre and Co Requisites: INTL 601
Equivalent course(s): none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Explain the importance of computer forensics in the field of information security.			
2. Differentiate between the various necessary digital forensic components.			
3. Examine digital evidence.			
4. Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.			
5. Analyze file system formats.			
6. Recover lost data.			
7. Examine secure deletion methods.			
8. Compare some different disk and forensic tools.			
9. Examine the role of digital forensics in public and private investigations.			

INTL 601 – Information Technology Auditing

You will learn about the concepts of auditing, controls and security in an Information Technology (IT) environment. You will study the following topics: general internal controls and their application, security, governance, standards, guidelines and regulations. You will examine methods and procedures used to assess the risks and evaluate controls over information systems in an organization.

Credit unit(s):	3.0
Pre and Co Requisites:	CSEC 603, CSEC 605
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Examine the fundamental auditing concept and concerns in an information technology (IT) environment.			
2. Evaluate internal controls used in information technology to meet business objectives.			
3. Analyze the best practices for internal controls as outlined in the standards from control objectives for information and related technologies (COBIT), committee sponsoring organizations of the Treadway Commission (COSO), international organization for standardization (ISO) and Information Technology Infrastructure Library (ITIL).			
4. Create a risk assessment to determine if the risk is being managed at an acceptable level in an Information Technology environment.			
5. Examine the requirements for compliance in laws and regulations such as health insurance portability and accountability act (HIPAA), Sarbanes-Oxley (2002) (SOX), personal information protection and electronic documents act (PIPEDA), and payment card industry data security standards (PCIDSS).			
6. Assess the general controls implemented to provide security in a specific IT environment and recommend improvements.			
7. Evaluate the various approaches to test the internal controls as implemented in various IT applications.			
8. Examine the best practices for implementing business continuity and disaster recovery.			
9. Examine the issues related to security and control for a wide range of IT technologies.			

PROJ 603 – Capstone Project

You will learn how to work in a group to plan and execute a major information technology (IT) project. You will manage and monitor the project and produce documentation to communicate effectively with your stake holders.

Credit unit(s):	3.0
Pre and Co Requisites:	CSEC 607, INTL 601
Equivalent course(s):	none

Use a checkmark (✓) to rate yourself as follows for each learning outcome **Competent:** I can apply this outcome without direction or supervision. **Learning:** I am still learning skills and knowledge to apply this outcome. **None:** I have no knowledge or experience related to this outcome.	**Competent**	**Learning**	**None**
1. Propose a project methodology.			
2. Research the technical and design aspects required to complete the project.			
3. Manage scheduling to ensure timely completion of the project.			
4. Monitor the progress of a project.			
5. Manage the quality of the project process.			
6. Manage the quality of project deliverables.			
7. Present the outcome of the project to stakeholders.			
8. Close a project.			