WHO'S MINDING YOUR BUSINESS?

SECURITY CHECKLIST

Self assessment tool for businesses and organizations.

BROUGHT TO YOU BY THE
WHITEHORSE CHAMBER OF COMMERCE
AND OUR CRIME PREVENTION PARTNERS

WELCOME

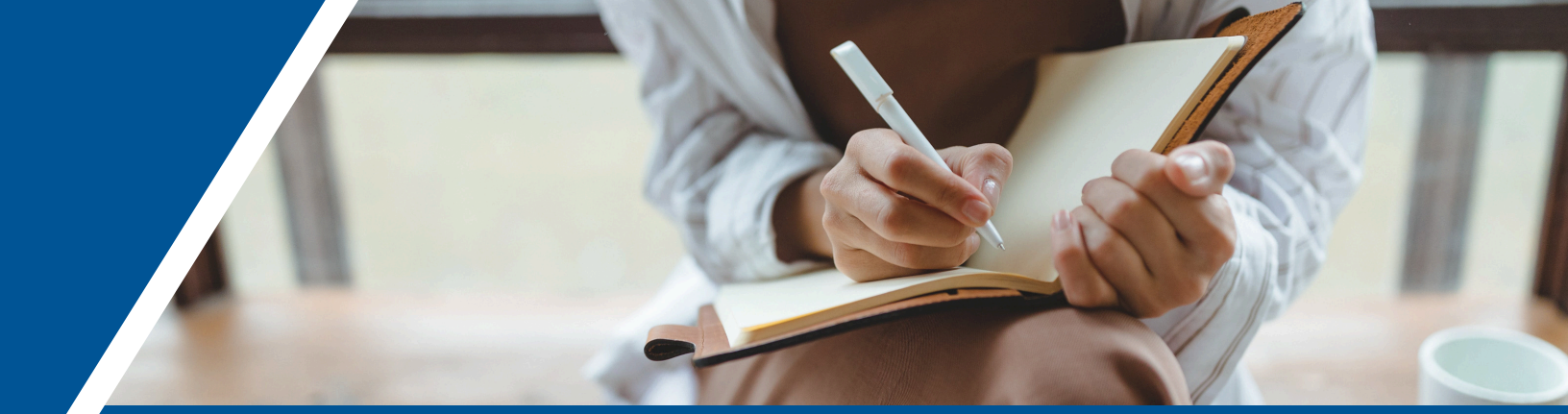
This security document has been developed specifically for the Yukon business community as a practical self-assessment tool, designed to help identify and address security vulnerabilities within businesses and organizations. By using this resource, business owners and employees can gain valuable insights into their security preparedness and take proactive steps to mitigate potential risks.

Crimes against businesses are often opportunistic rather than premeditated. Criminals look for weaknesses they can exploit, making it crucial to ensure that your business is as secure as possible. Reducing opportunities for crime not only deters potential offenders but also minimizes the impact of any incidents that may occur. A thorough security assessment allows you to take a strategic approach, identifying vulnerabilities and implementing measures that enhance the overall safety of your business.

This booklet is structured into 19 key sections, each featuring checklists that examine different areas of your business's security framework. You have the flexibility to follow the booklet in order or jump directly to sections addressing your most pressing concerns. However, completing all sections will provide the most comprehensive evaluation of your security measures.

Regular security assessments are essential for staying ahead of potential threats. By conducting these reviews periodically, you can proactively identify areas that require attention, ensuring your business remains resilient against crime and security risks.

If you would like to discuss this checklist, please don't hesitate to contact the Whitehorse Chamber of Commerce at 867-667-7545 or business@whitehorsechamber.ca. For your convenience a digital version of this booklet is also available at www.whitehorsechamber.ca



HOW TO USE THIS CHECKLIST

This checklist helps you find security weaknesses in your business or organization and take the necessary actions to address them. Here's how to begin:

- **Pick a section:** Start with the topic that concerns you most or follow the checklist in order for a complete review.
- **Answer Each Question:** check the corresponding N/A, Yes or No at the end of each question.
- **Calculate the Risk:** At the end of each section, use the fill-in-the-blank equation provided to calculate the risk to your business as a percentage.
- **Review Your calculations:** Use the percentages you generated to identify any high-risk areas needing immediate action and plan improvements.

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

- **Follow Recommendations:** Take steps based on your calculations, such as improving lighting, upgrading locks, or consulting a security professional.
- **Repeat Regularly:** Use the checklist regularly to keep your security updated and adapt to new risks.

The goal is to identify security measures that will make it harder for someone to exploit your business and increase the risk of these people getting caught.

TABLE OF CONTENTS

BUILDING EXTERIOR

LANDSCAPING

		N/A	Yes	No
1	Are fences around the building, exterior compounds and parking lots in good repair?			
2	Are fences low enough to provide an unobstructed view of the facility to minimize any potential hiding spots so that someone passing by can easily see inside the business?			
3	Is the fence free of loose objects, i.e. boxes, debris, garbage bins, lumber, etc.?			
4	Are all gates to fenced areas secured?			
5	Are trees, shrubs, flower beds, etc., far enough away from perimeter walls/floor windows to not provide hiding spots?			
	TOTALS			

Calculate your Risk Percentage for Landscaping using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(5 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUILDING EXTERIOR

VISIBILITY

		N/A	Yes	No
1	Is the business located within an area that provides high public visibility?			
2	Is the municipal address clearly marked, and does signage clearly identify your business to ensure that emergency services can quickly find it?			
3	Are all entrances, windows, the parking lot and the garbage area well-lit (i.e. are they bright enough to allow for facial recognition)?			
4	Do the exterior cameras work well with existing lighting to provide good image coverage?			
5	Are all exterior lights in these areas working?			
6	Are exterior lights housed in vandal-resistant housings?			
7	Are exterior lights placed high enough to be out of reach to prevent vandalism and tampering?			
8	Is there additional exterior lighting in areas that are vulnerable to black spots or hiding spots?			
9	Are windows and entrances free of obstructions (e.g., furniture, posters, or items that block visibility) to ensure clear views into the business from the street?			
10	Are all entrance doors clearly visible from either the parking lot or the street?			
11	Can you clearly see if someone is standing inside before you enter?			
12	Do you remove any furniture or items that might be used to sit on from outside your business during non-operating hours?			
13	Are mirrors or cameras installed on the corners of the building so, from the back doorway, an employee has a view of the sides and back of the building?			
14	Are windows clear of posters or signs that might block the interior view of the business?			
	TOTALS			

Calculate your risk percentage for Exterior Visibility using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(14 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUILDING EXTERIOR

DOORS, WINDOWS AND OTHER OPENINGS

		N/A	Yes	No
1	Is the ground floor of the perimeter walls free of exterior ladders or pipes leading to upper floor windows or rooftop?			
2	If exterior ladders that lead to upper-floor windows or rooftops are hard mounted to the wall, is the bottom secured by a steel plate and lock to prevent unauthorized climbing?			
3	During non-operating hours, do you put away any outside equipment (such as snow shovels) or other materialsthat might be used to break a window or gain access to your business?			
4	Do you secure or anchor outside items that are impractical to be put away during non-operating hours (such as picnic tables or other heavier or bulkier items) that might be used to break a window or gain access to your business?			
5	Are all perimeter doors self-closing?			
6	Are all perimeter doors either hinged on the inside or equipped with hinges that don't allow hinge pins to be removed from the outside?			
7	Are all perimeter doors equipped with latch guards to protect the latch?			
8	Are all entrance doors clearly visiblefrom either the parking lot or the street?			
9	Can you clearly see if someone is standing outside a door before you open it?			
10	Do all windows and doors have locks which are working and in good repair?			
11	Are all windows locked during non-operating hours?			
12	Are all windows, skylights and doors protected by strong frames and safety and shatterproof glass (e.g. laminated glass that protects against forced entry)?			
13	If necessary, can the door and window locks and safety bars be easily unlocked by employees to use as an emergency exit?			
14	If any changes are made to the locks and glass in doors and windows are there procedures to ensure the changes comply with building and fire codes?			
15	Are heating, ventilation and air conditioning ducts secured and at least 10 feet off the ground to prevent entry?			
	TOTALS			

Calculate your risk percentage for Doors, Windows and Other Openings using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(15 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUILDING INTERIOR

VISIBILITY

		N/A	Yes	No
1	Is the manager/staff office kept locked and restricted to limited authorized staff only?			
2	Are sensitive documents/information stored in lockable cabinets or safes only accessible to authorized staff?			
3	Are electronic files and communications protected from unauthorized access through the use of strong passwords which are regularly updated?			
4	Are sensitive documents that can be destroyed shredded with cross-cut or micro-cut shredders for better security as opposed to strip-cut shredders?			
5	Is lighting over all cash registers bright enough to ensure visibility from the street and other rooms?			
6	Are all interior rooms and hallways illuminated well enough to see anyone in them?			
7	Are there clear lines of sight between storage racks so anyone in a storage area can be seen?			
8	Can any employee in a storage area clearly see the doorway and be aware of whether another person is in the room?			
9	Is your storage area closed off from public view?			
10	Are hallways free of boxes or equipment that might provide hiding spaces?			
11	Are mirrors and/or cameras positioned strategically in long corridors so an employee can see along the entire length?			
12	Are height lines marked on the door frame or the wall to assist employees in accurately identifying individuals' heights during incidents?			
13	Are high-valued items securely locked away, and do you move articles of value away from the windows or doors during non-operating hours?			
14	Is access to the employee locker room or break room limited to employees?			
15	Are employees instructed to leave their valuables at home or in a locked locker?			
16	Do employees provide their own locks for their lockers, and do they use them?			
17	Are lockers and employee rooms monitored (both for security violations and employee safety)?			
	TOTALS			

Calculate your risk percentage for Interior Visibility using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(17 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

SECURITY SYSTEMS

KEYS AND NON-ELECTRIC LOCKS

		N/A	Yes	No
1	Does your business have a key control system with clear procedures for managing, storing, and recalling keys?			
2	Are all locks re-keyed periodically such as when keys are stolen/lost or after employees leave?			
3	If your business is equipped with non-electric push button code locks, do they come with a key override for a traditional key (in case of mechanical failure or if you forget your code)?			
4	Do employees only have access to keys during working hours?			
	TOTALS			

Calculate your risk percentage for Keys and Non-Electric Locks using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(4 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

SECURITY SYSTEMS

INTRUSION DETECTION SYSTEM

		N/A	Yes	No
1	Is your business equipped with an intrusion alarm with motion sensors?			
2	Are sensors (e.g., door contact and motion sensors) used at entrances and the facility's interior, including storage areas?			
3	Is your business equipped with glass break sensors near windows and doors?			
4	Are cash registers and safes equipped with security features such as tamper detection sensors or locks and seals that indicate if the machine has been accessed without authorization?			
5	Have you implemented two-factor authentication to access your point of sale (POS) system (i.e., a second form of verification, such as swiping an RFID card and then entering a unique PIN code)?			
6	Are panic/duress alarms installed at checkout counters?			
7	Are sensors and alarms adequately set?			
8	Are sensors and alarms maintained in working order?			
9	Are alarms tested regularly?			
10	Are employees trained in the policies and use of alarm and sensor systems?			
11	Is there a call-out list for the alarm, and is it updated regularly?			
12	Are all security systems and security-related renovations checked against fire and building code requirements?			
13	Do employees know what to do in the event of a false alarm or accidental triggering?			
	TOTALS			

Calculate your risk percentage for Intrusion Detection System using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(13 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

SECURITY SYSTEMS

ELECTRONIC ACCESS CONTROL

		N/A	Yes	No
1	Is your business equipped with electronic card access with electronic locks, keypad locks, electromagnetic locks or smart locks?			
2	If your business is equipped with electronic keypad locks, do they come with a key override for a traditional key (in case of mechanical failure or if you forget your code)?			
3	Are all access control readers in working condition?			
4	Are the procedures for making, storing, dispersing, and recalling all access cards and safes being used at the facility?			
5	Are access cards securely stored?			
6	Is the access control system programmed so that employees only have access during working hours?			
7	Are maintenance plans and lifecycle management plans in place for the Access Control System?			
	TOTALS			

Calculate your risk percentage for Electronic Access control using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(7 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

SECURITY SYSTEMS

CAMERAS

		N/A	Yes	No
1	Do the security cameras provide good image quality (e.g. capable of providing adequate facial recognition during both daylight and hours of darkness)?			
2	Are your security cameras capable of recording?			
3	Can your security cameras be monitored at your place of business?			
4	Are security camera recording devices kept in a secure location?			
5	Are security cameras live video monitored by a professional monitoring service?			
6	Are your cameras continuously live video monitored during working hours?			
7	Are your cameras continuously live video monitored during non-operating hours?			
8	Can your cameras be monitored via a smart system (e.g. via Wi-Fi smartphones or tablets)?			
9	Do cameras provide coverage at all access points?			
10	Do cameras provide coverage at cash handling locations?			
11	Are employees trained on how to operate the security cameras, including accessing and retrieving recordings if needed?			
12	Are your cameras equipped with motion-triggered recording capabilities?			
	TOTALS			

Calculate your risk percentage for Cameras using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(12 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

SECURITY SYSTEMS

CYBER SECURITY

		N/A	Yes	No
1	Does your business rely on centrally managed data centres or cloud services to handle your data processing and storage needs (e.g., point-of-sale systems, inventory management and other crucial operations)?			
2	If your business houses its own server room or network/data closet, is it secured and equipped with an alarm and a security camera?			
3	Is your door to a server room/data closet hinged on the inside or, if hinged on the outside, equipped with non-removable hinge pins?			
4	Do you update your software with patches and improvements when released by the software company?			
5	Do you run antivirus software and regularly scan systems for malicious files?			
6	Do you use two-factor authentication for all your computer systems? Are passwords kept secret and changed at least once every 90 days?			
7	Are security controls in place and used for all POS and back-office computer systems?			
8	Are your computer systems equipped with firewalls, antivirus and malware?			
9	Do you conduct regular visual inspections on each POS device to look for possible signs of tampering?			
10	Do you verify the identity of repair technicians and remain with staff during any work on POS devices in case of unannounced technical service visits?			
11	Do you utilize security tethers or cables to attach the POS devices to a fixed point on the counter or a secure stand to ensure their security?			
12	When not in use, do you store the POS devices under the counter or out of reach of customers?			
13	Do you keep backup POS devices locked to prevent unauthorized access?			
14	Do security cameras provide a clear view of POS devices and PIN pad terminals while ensuring they do not capture the PIN entered by customers?			
15	Do you train your employees to always log out and never share passwords or other information, including when walking away from the POS system?			
	TOTALS			

Calculate your risk percentage for Cyber Security using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(15 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS ASSETS

PROPERTY AND EQUIPMENT

		N/A	Yes	No
1	Is all property and equipment tagged or marked with an inventory number?			
2	Is there a written inventory that lists all equipment and supplies?			
3	Is the written inventory updated as needed and stored safely off the premises?			
4	Are employees assigned responsibility for the whereabouts and condition of equipment and property?			
5	Is the inventory inspected and counted on a regular basis?			
6	Are there written employee policies for personal use of equipment and property?			
	TOTALS			

Calculate your risk percentage for Property and Equipment using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(6 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%
Low Risk
Maintain existing measures

34–66%
Medium Risk
Address identified vulnerabilities

67–100%
High Risk
Take immediate action

BUSINESS ASSETS

SAFES

		N/A	Yes	No
1	Are safes equipped with secure one-way drop slots for deposits?			
2	Are safe combinations written down and kept in a secure location?			
3	Are safes secured to the floor or wall so they cannot be removed?			
4	Are safes kept locked at all times?			
5	If the safe is in the manager's office, is the office locked when the manager is not inside?			
6	Does your safe require biometric authentication (e.g. fingerprint verification) integrated with a time lock delay to ensure that only authorized users can attempt to open it?			
7	Is your safe kept in an area where it cannot be easily seen?			
8	Do you regularly maintain your safe to ensure it works properly?			
9	Are smart safes used that automatically count and validate cash as it is deposited, that provides real time tracking?			
	TOTALS			

Calculate your risk percentage for Safes using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total "NO" answers}}{\left(\text{Number of questions} - \text{"N/A" Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(9 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%
Low Risk
Maintain existing measures

34–66%
Medium Risk
Address identified vulnerabilities

67–100%
High Risk
Take immediate action

BUSINESS PRACTICES

GENERAL SECURITY

		N/A	Yes	No
1	Are policies in place against having former employees, or acquaintances and relatives of current employees, in the facility after closing or in restricted areas during business hours?			
2	Do you establish a maximum cash limit for your register? Once this limit is reached, is the excess promptly removed and securely stored in a safe?			
3	To deter theft, are signs posted indicating that the amount of cash in the register does not exceed a certain amount, that an alarm system protects the business and that employees cannot open the safe?			
4	Have employees been told not to give information about operating and security procedures to guests, telephone callers, outside contractors, and vendors?			
5	Are employees required to park far enough from the building so that they cannot quickly transfer stolen items to their vehicles?			
6	Are employee arrivals and departures restricted to specific times and certain doorways?			
	TOTALS			

Calculate your risk percentage for General Security using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(6 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS PRACTICES

CASH MANAGEMENT PROCEDURES

		N/A	Yes	No
1	Is access to cash registers limited to certain employees?			
2	If electronic cash registers with digital locks are used, are employees provided with their own unique code for access?			
3	Are employees who handle cash transactions trained in cash-handling procedures?			
4	Are there written employee policies for handling money and receipts?			
5	Have employees signed your cash handling policy statement?			
6	Are all employees who handle payments trained to recognize if a form of payment is fraudulent?			
7	Are employees trained in what to do if they suspect a form of payment to be fraudulent (e.g. request picture ID)?			
8	Are employees instructed to check the signature area on the back of each credit/ debit card? (Note: While many credit/debit cards no longer require you to sign the back of credit/debit cards due to newer technology, some customers instead write “Please check for ID” in this area?			
9	Are managers required to oversee all corrections of error in cash register entries?			
10	Are employees who handle cash instructed not to give cash back on cheques, credit cards or gift cards?			
11	Before opening, are cash registers supplied with only a minimum amount of cash?			
12	Are receipts generated for each cash register transaction?			
13	Is one transaction completed and rungout before another is begun?			
14	Are cash drawers to all registers kept closed and locked between transactions?			
15	Are “overrides” and “voids” on point-of-sale computers and cash registers approved by managers before transactions are completed?			

		N/A	Yes	No
16	Are receipts (paper or electronic) reconciled with the cash in the drawer at least once each shift?			
17	Are cash and credit card receipts removed from the facility or securely locked away after each business day?			
18	Is money counted only behind a closed, locked door?			
	TOTAL			

Calculate your risk percentage for Cash Management Procedures using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total "NO" answers}}{\left(\text{Number of questions} - \text{"N/A" Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(18 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS PRACTICES

ACCOUNTING PROCEDURES

		N/A	Yes	No
1	Are cheques and deposit slips locked up?			
2	Is access to checks, deposit slips and receipts divided up between two or more managers or employees to provide a system of checks and balances in accounting procedures?			
3	Are blank cheques kept in a secure place?			
4	Are two signatures required on all cheques?			
5	Is petty cash kept to a minimum and secured in a manager's office or safe?			
6	If paychecks and gift certificates are generated by a computer on-site, are security paper and/or security features used to prevent illegal duplication or alteration?			
7	Do your gift certificates or coupons feature unique, trackable codes that allow monitoring from issuance to redemption, ensuring they are used only once?			
8	Are digital accounting systems secured with strong passwords and updated regularly?			
9	Do you back up financial data to secure, off-site locations or the cloud?			
10	Is access to your accounting software limited to authorized personnel only?			
11	Is your accounting software protected with two-factor authentication?			
12	Are regular audits conducted to check for unauthorized access or discrepancies?			
	TOTALS			

Calculate your risk percentage for Accounting Procedures using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(12 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS PRACTICES

BANK DEPOSITS

		N/A	Yes	No
1	Does a manager oversee the preparation of money for bank deposits?			
2	Are deposits made by different managers or employees to ensure accountability?			
3	Are deposits made daily so that cash does not build up to high amounts?			
4	Are deposits sent to the bank by armoured car or bonded messenger?			
5	Is money to be deposited into the bank brought in a package that does not look like a bank deposit bag?			
6	Are tamper-evident deposit bags with unique serial numbers or bar codes used for bank deposits?			
7	If the manager or an employee takes deposits to the bank, is the route, day and time of bank deposits varied constantly to prevent predictable patterns that a theif might follow?			
8	While at the bank, do employees know not to talk to anyone except the teller?			
9	If a night deposit slot or box at the bank is used after hours, do employees know they should not approach it if other people are standing around?			
10	Do employees feel comfortable reporting any unusual occurrences they may notice on the way to or while they are at the bank?			
11	Are bank receipts received and maintained on file for all deposits?			
	TOTALS			

Calculate your risk percentage for Bank Deposits using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(11 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS PRACTICES

OPENING AND CLOSING

		N/A	Yes	No
1	Are security practices integrated into procedures for opening and closing?			
2	Are there written policies and procedures for employees who open and close the facility?			
3	Is a manager always present for opening and closing?			
4	Are employees trained in opening and closing procedures?			
5	Do employees work in teams to open and close?			
6	Before entering, do employees inspect the exterior of the building for signs of a break-in or vandalism?			
7	Do employees ensure no one is loitering on the property before opening the doors or locking up at closing?			
8	Do employees lock the door behind them and keep it locked until it is time to open for business?			
9	Are employees instructed to only allow scheduled employees to enter the building before opening hours?			
10	Do employees complete an inspection of the business 30 minutes before closing and after closing to see that no one is hiding inside the business, including in the restrooms/washrooms?			
11	Are employees instructed not to let in anyone after closing?			
12	Are all doors locked promptly at closing and kept locked until all closing employees leave?			
	TOTALS			

Calculate your risk percentage for Opening and Closing using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(12 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS PRACTICES

TAKING OUT THE TRASH

		N/A	Yes	No
1	Is trash taken out by two or more employees together?			
2	Is the back door (door used to take out the trash) closed and locked after the trash is taken out?			
3	Is trash only taken to the outside dumpster before dark?			
4	Are trash cans, garbage containers, and empty boxes inspected by the manager to ensure that employees are not taking out supplies or equipment?			
5	To maintain a professional appearance and to reduce the likelihood of unauthorized individuals hiding or loitering, are dumpster and trash enclosure areas kept neat, clean and uncluttered?			
6	Are dumpsters and trash enclosures kept secure to prevent unauthorized access?			
	TOTALS			

Calculate your risk percentage for Taking out the Trash using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total "NO" answers}}{\left(\text{Number of questions} - \text{"N/A" Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(6 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

BUSINESS PRACTICES

WORKING WITH VENDORS

		N/A	Yes	No
1	Is vendor access limited to specific times, entrances and areas within the building?			
2	Are vendors supervised by a specific employee or manager while they are on the premises?			
3	Are manager-approved purchase orders required before ordering supplies?			
4	Are all deliveries checked against purchase orders before being received?			
5	Are all shipments double-checked against their invoice before packing and delivery?			
	TOTALS			

Calculate your risk percentage for Working with Vendors using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\quad}{\left(5 - \quad\right)} \right] \times 100 = \quad \%$$

0–33%
Low Risk
Maintain existing measures

34–66%
Medium Risk
Address identified vulnerabilities

67–100%
High Risk
Take immediate action

MANAGEMENT PRACTICES

TRAINING AND MONITORING EMPLOYEES

		N/A	Yes	No
1	Are employees made aware of available trauma counselling and support services, such as those provided by the Yukon Workers' Compensation and Health and Safety Board, in the event of a traumatic workplace incident, such as a workplace accident or violent incident?			
2	Do you have written security policies?			
3	Do all employees receive training in security procedures, security systems and alarms, and security policies?			
4	Are employees reminded of their responsibilities concerning security on a regular basis?			
5	Are employees made to feel comfortable in reporting security violations to management?			
6	Are employees provided with recognition or incentives for following security rules and reporting security violations?			
7	Are employees trained in basic theft prevention practices (such as greeting each customer who enters the business with eye-to-eye contact)?			
8	Are employees trained to deal with emergencies (such as what to do in the event of a robbery)?			
9	Do you record all incidents in a log?			
10	Do you report all crimes to the RCMP?			
	TOTALS			

Calculate your risk percentage for Training and Monitoring Employees using the following formula:

$$\text{RISK PERCENTAGE} = \left[\frac{\text{Total “NO” answers}}{\left(\text{Number of questions} - \text{“N/A” Answers}\right)} \right] \times 100 = \%$$

Fill in the blanks from your answers above and calculate the percentage.

$$\text{RISK PERCENTAGE} = \left[\frac{\square}{\left(10 - \square\right)} \right] \times 100 = \square\ \%$$

0–33%	34–66%	67–100%
Low Risk	**Medium Risk**	**High Risk**
Maintain existing measures	Address identified vulnerabilities	Take immediate action

RECOMMENDATIONS

RISK VALUES

Now that you have a calculated risk percentage a common approach before deciding on the next steps is determining Risk Acceptance. As a rule, however, risk values in the high range generally require immediate action, while risk values in the low range are usually acceptable. Those in the medium range would likely require careful examination to determine their relative acceptability.

Interpretation and Next Steps

Upon completing this Security Checklist, or a relevant section, businesses should consider the following next steps based on their score range:

Low Risk – Retain existing safeguards and conduct annual self-assessments to ensure existing systems and practices are kept up to date.

Medium Risk - Identify the highest vulnerabilities from the checklist and initiate safeguards to reduce the risk. Consider having a security consultant who can conduct a formal Risk Threat Risk Assessment and provide recommendations on how to mitigate the risk.

High Risk - Initiate safeguards to reduce the risk and consider engaging with a security consultant who can conduct a formal Security Risk Assessment and provide recommendations on mitigating any high risks and vulnerabilities identified.

RESOURCES

CITY OF WHITEHORSE

Report a Problem: https://www.whitehorse.ca/contact-us/report-a-problem/

Contact the City: https://www.whitehorse.ca/contact-us/

Bylaw Services: phone: 867-668-8317 or email: bylaw.services@whitehorse.ca

City of Whitehorse Trouble Line: 867-667-2111

CRIME STOPPERS YUKON

Report a Crime: 1 (800) 222-8477

Report a Crime online: https://www.p3tips.com/Drill.aspx

Download Crime Stoppers App: https://www.p3tips.com/community/index.htm

---

WHITEHORSE RCMP

Address: 4100 4th Avenue, Whitehorse, YT Y1A 1H5

For emergencies please call **9-1-1** or your local emergency number

Online reporting: https://report.rcmp.ca/whitehorse/en

Non emergency line: 867-667-5555

WHITEHORSE CHAMBER OF COMMERCE - SAFETY COMMITTEE

Address: 101, 302 Steele Street, Whitehorse YT Y1A 2C5

Phone: 867-667-7545

Email: business@whitehorsechamber.ca

THANK YOU

The Whitehorse Chamber of Commerce would like to thank all the contractors and stakeholders for their input, collaboration and support in the creation of this updated document.

Whitehorse
THE WILDERNESS CITY

CRIME STOPPERS
YUKON COMMUNITY ASSOCIATION

Yukon

Yukon

Whitehorse Chamber of Commerce
101-302 Steele Street, Whitehorse YT Y1A 2C5
E: business@whitehorsechamber.ca
P: (867) 667.7545

whitehorsechamber.ca

2ND EDITION MARCH - 2025