The model that I will be proposing for this audit will be a compilation of two frameworks: NIST SP800- 53r5 and NISTIR 7621r1. The proceeding checklists consists of 11 items that have been deemed as crucial to the safety of the customer's privacy and information.

* NIST SP800-53r5:
  + AC-6 Least Privilege
  + AC-10 Concurrent session control
  + AC-17 Remote access
  + AC-19 Access control for mobile devices
  + AC-21 Information Sharing
  + AT-1 Policy and Procedure
  + AT-2 Literacy training and awareness
* NIST 7621r1:
  + 3.2 Protect
  + 3.3 Detect
  + 3.4 Respond
  + 3.5 Recover

The NIST 7621r1 provides a broader over-encompassing approach that helps guide the business into the type of security that clamps down on any intrusion; it takes much broader approach, but it is both equal parts prevention and threat mitigation. The NIST SP800-53r5 provides a more targeted approach at prevention, providing numerous limitations on the user along with awareness and threat identification. The model that I will be providing encompasses both frameworks but emphasizes more on prevention, and awareness. I will first cover the NIST SP800-53r5’s checklist explaining why each item was selected, and follow with NIST 7621r1, and provide my reasoning for its respective items.

AC-6 Least Privilege:

Users should only be allowed to use privileged software based on their role in the business. By limiting the amount of privilege that a user has access to, if, theoretically, the user’s account was compromised, it would limit the number of systems that are impacted and could be used for malicious purposes. Within the least privilege control, we could also employ enhancement 3 which includes authorizing network access commands for certain operational needs while also documenting the reasoning behind such needs.

AC-10 Concurrent Session Control:

A small business should take care of how many concurrent sessions its employees have access to based on the role of the employee. By closely monitoring the attempts that an employee has made in having various sessions open, a small business can use this as a detection measure to see if high levels of attempts are caused by a compromised user, this also limits the attackers window of operation as it would be easy to trigger such a detection measure.

AC-17 Remote Access:

As more and more employers have shifted to remote work, it can be deduced that an attacker will attempt to compromise a user’s account using the employee’s personal computer, as a personal device has less security than that of an enterprise device. We can further strengthen this control by implementing enhancement 10 (Authenticate remote commands) by implementing a two-factor authentication process that requires an employee to input a pin and a token so that specific commands and logins can be verified; this provides strong protection in assuring that an employee and not an attacker is the individual that is logging in.

AC-19 Access Control for Mobile Devices:

Personal handheld devices are the most prevalent form of communication, and if an attacker was to compromise an employee’s mobile device, the attacker would have an array of sensors and tools that could be used to spy and further advance their attempts of intrusion. Implementing policies that limits mobile device usage can further enhance the security of a small business the rationale behind such policies is due to the possibility of employees not having the lates security patches updated to their mobile devices, such lack of patches can cause an attacker to exploit the employee’s mobile device and use it to compromise any system an employee connects their device to.

AC-21 Information Sharing:

Information sharing can be an easy oversight, if an employee has the privilege to send emails with sensitive information outside of the organization, this can cause huge regulatory issues, along with providing attackers the ability to send mass amounts of information outside of the business without raising suspicion. This can further be enhanced to include the restriction of external communication, only specified users can have access to send out external emails which would require that the emails sent out along with the users account have extra scrutiny in case the account is ever compromised.

AT-1 Policy and Procedure:

This control falls under the category of awareness and training, and the purpose of such a control is to build policies that reduce the possibility of an attacker compromising a system or network. Management can create awareness information and develop training materials that users can learn upon.

AT-2 Literacy Training and Awareness:

The purpose of such a control is to raise employee awareness of disguised cybersecurity threats. Human error is usually the biggest weakness, and for a small business, it can be easier to assure that most if not all employees are aware of the tactics used to compromise a network. By having quarterly training sessions and knowledge checks along with mock attack, the human error can be greatly reduced.

The following list of items are controls listed from the NIST 7621r1 framework that have been incorporated into this model.

3.2 Protect:

This area of the NIST 7621r1 goes hand in hand with the items listed in NIST SP800-53r5. Protecting information that customers have trusted the small business with is paramount to success and trust that the company has acquired. Particularly the subitem “User encryption for sensitive business information”. If a system or network was ever to be compromised, the information would be useless to the attacker, and would be a type of failsafe that if all other forms of repel were to fail, the information that was stolen would be rendered useless. Another helpful item would be to secure wireless access points and networks, in doing so, the information that is trafficked in the network would be safe from an attacker trying to intercept any information.

3.3 Detect:

One of the most important aspects of security is the detection of an attack or compromised system/network. By implementing anti-virus, -spyware, and -malware programs, detection can be done quickly and efficiently, this reduces the time that an attacker can has inside of a system or stops an attack altogether if implemented appropriately along with other safeguards. Including the ability to log any activity that has been done in a system can also help to make sure that nothing suspicious is overlooked and at the very least find out how the attack was done.

3.4 Respond:

This item is important as it acts as a guide on what to do if an attack was successful. By creating a plan on who to contact, the appropriate steps to take to quickly stop an attack, and when to involve authorities should all be carefully planned out, without a guide, a small business can cause its employees to quickly panic and possibly alert the intruder that the business became aware of the attack, this can then deter the possibility of ever tracing and apprehending the attacker.

3.5 Recover:

One of the most important items on this list is the ability to recover anything that has been compromised. Ransomware attacks are more rampant as it allows an attacker to hold systems hostage while demanding a ransom. This directly impacts the business as attackers usually ask for astronomical amounts that could bankrupt a small business. If backups were to be made, the ransomware attack would be rendered useless. There are various ways to store backups, some locally or via other businesses that provide such services. We can further enhance this control by making sure that all backups are fully encrypted as to assure that if backups were to be compromised, sensitive information would be protected.