CIS Controls Roadmap for IG1 Enterprise

This project will demonstrate how to use the CIS Controls Guide to protect an IG1 level enterprise from cybersecurity threats. An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and mainly surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

In this project I will be using the most up-to-date CIS Controls (Version 8) to provide an example walkthrough for a fictional IG1 sized company which I will refer to as Albatross Insurance or simply Albatross. I will be approximating the technology that a business this size would have in use. The process would obviously be more thorough with more safeguards for an IG2 or IG3 level company that has greater security needs.

For the sake of brevity, the assets and operational capacity of this fictional company will be much smaller than a typical IG1 company therefore each safeguard will have less complexity than a typical IG1 enterprise would. This is meant more as an exercise to show how you would approach implementing the safeguards when evaluating a business under the CIS Controls.

Albatross will only have two employees named Dick and Jane Garfunkel. They are old school and only use technology when absolutely necessary to complete their jobs. I was hired to give them a secure baseline that can be maintained and easily expanded as their business grows. I will also be in charge of their incident response should a breach occur.

Control 01: Inventory and Control of Enterprise Assets

1.1 Establish and Maintain Detailed Enterprise Asset Inventory

I would conduct a thorough review of all the hardware assets of Albatross and document them in as much detail as possible. Additional criteria would be added for a company with more employees to keep things organized like Department Name. There are many types of software for tracking assets, such as Asset Panda or Solarwinds, or I could simply create a table myself like I have done in this example.

Asset Name	Asset Type	Asset Owner	IP Address	MAC Address	Network Connection Approval
Acer P225HQL	Monitor	Dick Garfunkel	N/A	N/A	N/A
AOC LM729	Monitor	Jane Garfunkel	N/A	N/A	N/A
Dell Optiplex 9020M	Workstation	Dick Garfunkel	192.168.2.12	5E:71:F4:c1:11:00	Yes
Dell Optiplex 9020M	Workstation	Jane Garfunkel	192.168.2.13	5E:71:F4:c1:16:24	Yes
Dell 1130n	Printer	Dick Garfunkel	192.168.1.90	00:0e:8e:71:b7:56	Yes
Asus RT-AC66U	Router	Dick Garfunkel	192.168.1.1	00:6a:8e:71::42:2w	Yes
Samsung Galaxy Note 9	Cell Phone	Dick Garfunkel	192.168.1.8	4w:21:32:u7:7p:03	Yes
Samsung Galaxy Note 9	Cell Phone	Jane Garfunkel	192.168.1.9	4w:21:32:k9:7p:8e	Yes

1.2 Address Unauthorized Assets

Run an arp -a scan weekly to identify assets that are connected to the network and remove any that are not approved on the hardware list. Devices can be added to the hardware list as needed.

Control 02: Inventory and Control of Software Assets

2.1 Establish and Maintain a Software Inventory

This safeguard is essentially the same as tracking the hardware assets but for software. I would want to keep track of how many licenses and instances of the software were installed on different machines as well as when they were installed. Ideally I would use a program designed to do this with features to ensure software is kept up to date but for this example I will use a table. Software inventory would be updated monthly.

Software	Manufacturer	Category	Owner	Purchased	Installed	Install Date
Windows 10	Microsoft	Operating System	Dick Garfunkel	2	2	6/7/2018
Photoshop 21.0	Adobe	Desktop	Jane Garfunkel	1	1	9/19/2019

Salesforce CRM	Salesforce	Desktop	Dick Garfunkel	2	2	6/7/2018
Apache HTTPD 2.4	Apache	Web Server	Dick Garfunkel	1	1	6/7/2018
Android 8.1 Oreo	Google	Operating System	Dick Garfunkel	2	2	9/15/2020

2.2 Ensure Authorized Software is Currently Supported

I would make sure that only currently supported software was authorized for the enterprise system. If software is necessary for operations but unsupported I would document that risk to cover myself and make sure Albatross understood the risk acceptance. I would review the software monthly or whenever new software is added. In this example all software is supported.

2.3 Address Unauthorized Software

I would remove software that was unauthorized or document the exception. This would take place monthly. In this example all software is authorized.

Control 03: Data Protection

3.1 Establish and Maintain a Data Management Process

Albatross Insurance deals in property insurance and is required by law to keep records for six years after their expiration date of the policy. This will apply to all data collected about customers and their policies. This data contains Personally Identifiable Information (PII) and will be classified with high sensitivity. After six years have elapsed after the expiration date, the data will be erased from the CRM and any paper documents will be shredded.

Dick Garfunkel will operate as the data owner and will ultimately make decisions on how the data is handled on a day to day basis around the office. The data management process will be reevaluated annually.

3.2 Establish and Maintain a Data Inventory

The policy and customer data will be accessible in the CRM. This data will also be downloaded to a backup local encrypted hard drive and printed off into paper records. The hard drive will be kept in a locked safe on the Albatross premises. These paper records will be kept in the Garfunkel's locked storage facility outside their home so that a disaster at the office doesn't wipe out all the data. A master list cataloguing the paper records will be stored with them as well.

The inventory will be catalogued annually or when a major business change occurs.

3.3 Configure Data Access Control Lists

Dick and Jane are both authorized to access all customer data at Albatross. They will have full access permissions to local file systems, databases, and applications.

3.4 Enforce Data Retention

As laid out in the Data Management Process above, the data will be retained in all forms for 6 years after the policy expiration date. At that time it will be deleted or destroyed.

3.5 Securely Dispose of Data

After the 6 years have expired the data will be erased from the CRM and local hard drive. The paper documents will be shredded.

3.6 Encrypt Data on End-User Devices

The local hard drive on the Windows workstations will be encrypted with Windows BitLocker. The Samsung Galaxy Note 9 phones would be encrypted in the Settings under Security.

Control 04: Secure Configuration of Enterprise Assets and Software

4.1 Establish and Maintain a Secure Configuration Process

I would use the CIS Benchmarks Program to download the appropriate configuration for Windows Desktop and configure it to those standards. I would use the vendor specific guides to make sure both Adobe Photoshop and Salesforce CRM had the highest security configurations necessary. I would encrypt the Android devices in the settings menu. I would then update the documentation annually or whenever a large change in the organization occurred.

4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure

I would use the vendor specific guides to make the Dell workstations/printers and Asus router configured to the highest security standards. These configurations would be reevaluated on a yearly basis or when major changes occurred.

4.3 Configure Automatic Session Locking on Enterprise Assets

Operating systems will lock after 10 minutes of inactivity. The cell phones will require fingerprint scans to activate.

4.4 Implement and Manage a Firewall on Servers

Albatross is small and just uses shared drives on the Google Cloud so they do not have a local server. They manage privacy settings in Google to make sure documents are not accessible to outside actors. In a larger company with dedicated servers, the firewall guarding the servers would be restricted to allow only approved ports and protocols.

4.5 Implement and Manage a Firewall on End-User Devices

A host-based firewall must be installed on both workstations with a default-deny rule that drops all traffic except HTTPS port 443. Windows Defender includes a firewall as part of Windows 10 so I would configure that free firewall to enable the rule described above.

4.6 Securely Manage Enterprise Assets and Software

This was mostly covered in 4.5 but would expand to include firewall protection on the router so that the network facing printer can't be compromised. The default-deny rule on the workstation firewall will keep a low level operation like this secure.

4.7 Manage Default Accounts on Enterprise Assets and Software

Default accounts have been disabled on both workstations. Dick and Jane both have administrator account privileges on their own workstations and they are password locked out of the other user's workstations. Jane is the only one who uses Photoshop so Dick does not have access to her account. The Salesforce CRM software has an individual account for each of them so they can keep track of their own clients. Even though they are married and share a business they are competitive and like to keep that separated.

Control 05: Account Management

5.1 Establish and Maintain an Inventory of Accounts

The only accounts used in this organization are Dick and Jane's on their respective workstations. For a larger organization I would create a spreadsheet to keep accounts organized with information such as their name, username, start/stop dates, and department. I would check the status of these accounts every 45 days to make sure they are still authorized.

5.2 Use Unique Passwords

Dick and Jane would use multi-factor authentication on their cellular devices with fingerprint scanners and pins. They would have 14-character complex passwords on their workstations. They would be required to change these passwords every 45 days and would not be able to repeat passwords for 5 cycles.

5.3 Disable Dormant Accounts

I would disable dormant accounts after 45 days of inactivity or immediately upon termination of an employee. Albatross used to have a third employee named Chaz Garfunkel but he was terminated and his account was disabled.

5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts

The only accounts active on these workstations are administrator accounts so there is no need to downgrade privileges on user accounts. For a larger organization the user accounts would be limited to only access things required to complete tasks for their specific jobs, such as internet browsing and email.

Control 06: Access Control Management

6.1 Establish an Access Granting Process

Albatross is small now but they are always looking to add more talent. In the event of a new hire I would assign the new employee access based on their job. Currently everyone has Administrator access but if they hired a secretary to lighten the load that employee would have a basic user account with limited privileges. We would adhere to a role-based access control model. For a larger company with established roles and responsibilities this process would be automated.

6.2 Establish an Access Revoking Process

Accounts would be immediately disabled upon termination of an employee. Since this industry might require records dating back 6 years, user accounts would be disabled rather than deleted to preserve the audit trail. Once again, in a larger company this process would be automated.

6.3 Require MFA for Externally-Exposed Applications

Albatross would use multi-factor authentication for Salesforce CRM and the Apache web server. A larger company would have more web facing applications and I would use packet and log inspection to make sure these were not compromised.

6.4 Require MFA for Remote Network Access

Albatross does not allow remote network access but for a larger company that needed this it would be enabled.

6.5 Require MFA for Administrative Access

This is not of the utmost importance for Albatross but would become critical for a larger organization. This would apply to all enterprise assets both on-site and through third-party providers.

Control 07: Continuous Vulnerability Management

7.1 Establish and Maintain a Vulnerability Management Process

I would scan the Albatross network with Nessus every 3 months and patch any significant vulnerabilities found at that time. Vulnerability scans will be performed whenever significant enterprise changes occur or high profile vulnerabilities are discovered and reported in the community.

7.2 Establish and Maintain a Remediation Process

I would use the NIST Common Vulnerability Scoring System (CVSS) to determine which vulnerabilities require immediate intervention. Critical and High risk scores will be immediately dealt with and Medium risk scores will be handled as time allows. The vulnerabilities that we have found and have left unresolved will be reevaluated every month to make sure they do not pose a more significant threat to the operation.

7.3 Perform Automated Operating System Patch Management

Operating system updates will be applied automatically as they are released and will be manually checked monthly.

7.4 Perform Automated Application Patch Management

Application updates will be applied automatically as they are released and will be manually checked monthly.

Control 08: Audit Log Management

8.1 Establish and Maintain an Audit Log Management Process

Log management is not a paramount concern at Albatross but it is still important for any business. They do not produce enough traffic to justify a centralized logging server like a larger company would typically have. Albatross does not want to spend money on this part of their business so they will be using OSSIM, which is open source, as their SIEM.

Albatross will save system logs to keep track of system process start/end times, crashes and things of that nature to keep their workstations running smoothly. These logs will be deleted weekly due to limited storage capacity. Audit/access control logs are not really a concern since both users are admins on their workstations but they will also be kept for a week in case something strange occurs. These logs will only be reviewed in the event of an incident. These protocols will be reevaluated annually.

8.2 Collect Audit Logs

Audit logging will be enabled and kept for a week before deletion per the audit log management process.

8.3 Ensure Adequate Log Storage

Due to the limited amount of log events produced and short amount of storage time local storage will be adequate for this log management process.

Control 09: Email and Web Browser Protections

9.1 Ensure Use of Only Fully Supported Browsers and Email Clients

Albatross uses Google Workspace for all of their online business applications. This transfers the heavy burden of security to a company more well equipped to handle the constantly changing environment of cybersecurity. Dick and Jane will install recommended security updates as they become available and are prompted to by both Google Chrome and Gmail. This will ensure the most up-to-date security measures are in place for both the browser and email client.

9.2 Use DNS Filtering Services

Google Chrome has a feature called Secure DNS that will be enabled on Dick and Jane's workstations. Chrome's Secure DNS feature uses DNS-over-HTTPS to encrypt the DNS communication, thereby helping prevent attackers from observing what sites you visit or sending you to phishing websites.

For a larger company it might be prudent to create your own enterprise policies regarding DNS filtering but for Albatross it makes more sense to leave that to the experts.

Control 10: Malware Defenses

10.1 Deploy and Maintain Anti-Malware Software

Albatross uses Windows 10 as their operating system which includes Windows Defender. This is a robust anti-malware solution that is frequently updated with the latest threats. Dick and Jane do not want to spend more than necessary so we have decided that this is sufficient malware protection when fully enabled. A larger enterprise could certainly benefit from additional third party software but this should be good enough for Albatross.

10.2 Configure Automatic Anti-Malware Signature Updates

Windows Defender has been configured to automatically download the latest signature updates to ensure full protection to known vulnerabilities at all times.

10.3 Disable Autorun and Autoplay for Removable Media

Autorun and Autoplay have been disabled for all removable media in the AutoPlay Settings of Windows 10.

Control 11: Data Recovery

11.1 Establish and Maintain a Data Recovery Process

This control works in tandem with control 3.1 when we established a Data Management Process. As stated earlier, the policy and customer data would be downloaded to a backup local encrypted hard drive and from this drive it could be fully restored in the event it was lost or corrupted. This data would be top priority to restore should anything happen to the CRM containing it.

This policy would be reviewed and updated annually or for any significant business changes.

11.2 Perform Automated Backups

The CRM customer and policy data would be configured to automatically backup at the end of each day. A larger organization would produce too much data for this to be feasible but for a small operation like this it will work fine.

11.3 Protect Recovery Data

This was laid out in control 03 but the encrypted backup hard drive would be separated in a locked safe. The paper documents being kept off site would provide another level of data separation and could be used to rebuild the company data in the event of a catastrophic event at the company headquarters.

11.4 Establish and Maintain an Isolated Instance of Recovery Data

This control was exactly laid out in 11.3 with the backup drive in the safe and the off site paper data. That is plenty of isolation.

Control 12: Network Infrastructure Management

12.1 Ensure Network Infrastructure is Up-to-Date

All hardware will be reevaluated on a yearly basis to ensure it is still functioning at an acceptable level. Software versions should be automatically enabled to update for all programs but they will be checked on a monthly basis and updated manually if they are not the correct versions.

IG2 and IG3 enterprises will require much more detailed Network Infrastructure Management safeguards but in this basic example of CIS Controls implementation we do not need to address them.

Control 13: Network Monitoring and Defense

IG1 level enterprises are not required to perform any safeguards in this control to achieve a passing security level. Most companies of this size simply don't have the resources to implement this control but if they do they would be wise to do so. This would include things like implementing a SIEM, a NIDS or NIPS, and managing access control for remote access. Definitely things I would want if I were in control of a business's security but not necessary for Albatross.

Control 14: Security Awareness and Skills Training

14.1 Establish and Maintain a Security Awareness Program

As anyone in the cybersecurity industry knows, people are the weakest link in an enterprise's defense. A security awareness training program would be much more robust at a larger organization but Albatross can certainly benefit from it as well.

Annual training would be conducted to refresh old information and also present new threats that have been growing for the past year. Periodic additional information concerning cybersecurity trends would be shared with Dick and Jane Garfunkel via email. Albatross would also be subject to occasional false phishing attacks to ensure they are on their toes.

The following safeguards are mostly self explanatory but I want to include them to show the whole security awareness picture for an IG1 enterprise.

14.2 Train Workforce Members to Recognize Social Engineering Attacks

Workers would be trained on social engineering attacks such as phishing, tailgating, and spam.

14.3 Train Workforce Members on Authentication Best Practices

This training would include things like multi-factor authentication, password complexity, credential management, and not sharing passwords between enterprise and personal accounts.

14.4 Train Workforce on Data Handling Best Practices

Training would include how we are storing customer data on the encrypted hard drive and procedures for printing off and transferring paper records to the off site facility. Would also emphasize not to share this sensitive data under any circumstances.

14.5 Train Workforce Members on Causes of Unintentional Data Exposure

These causes would include mis-delivery of sensitive data, losing a cell phone, and accidentally publishing PII online.

14.6 Train Workforce Members on Recognizing and Reporting Security Incidents

Workers would be instructed to point out potential phishing incidents, suspicious individuals trying to physically gain access to the building, and other things of that nature. Incidents would be reported to Dick Garfunkel.

14.7 Train Workforce on how to Identify and Report if Their Enterprise Assets are Missing Security Updates

Workers should understand alerts indicating software is not up-to-date and run that up the chain of command to the IT department, or in this case, Dick Garfunkel. This will help catch any failure in automatic updating procedures.

14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

This doesn't really apply to Albatross since no work is done remotely but it would include guidance to ensure that home network infrastructure is securely configured for remote workers in a larger organization.

Control 15: Service Provider Management

15.1 Establish and Maintain an Inventory of Service Providers

A common weak link for attackers to exploit is third party service providers. Companies place a lot of trust handing over data to these providers and can't really do much to guarantee it is being handled properly. Like all companies, Albatross must keep track of who else is handling their data and be able to resolve any issues with them that might arise from them being breached.

This documentation can be handled in a spreadsheet. The classifications below refer to the impact of a service outage or data breach at this level and will be either High, Medium, or Low. This classification does NOT indicate the likelihood of a breach.

Service Provider	Classification	Contact
Google Suite	High	1-650-206-5555
Salesforce CRM	High	1-800-667-6389
Google Cloud	High	1-855-817-0841

Control 16: Application Software Management

This control does not apply to Albatross because they do not have an application for their business and have no plans to develop one in the future. It is not a requirement for an IG1 level company to have this control under the CIS guidelines.

Control 17: Incident Response Management

17.1 Designate Personnel to Manage Incident Handling

Albatross does not have an in house security team so I would be in charge of their incident handling response. I would first inform Dick Garfunkel of the issue after the breach was isolated then I would inform any third party that was affected. This policy would be reviewed annually. In a larger organization this safeguard would have many more levels.

17.2 Establish and Maintain Contact Information for Reporting Security Incidents

This safeguard involves all the stakeholders that would be affected by the security incident as well as parties that might be part of the remediation effort. Albatross would have a fairly simple list of groups including Dick Garfunkel, law enforcement, third party vendors who might be involved, and the customers whose data has been affected. A larger organization would possibly have cybersecurity insurance and they would need to be alerted as well. These contacts would be verified annually to make sure they are up to date.

17.3 Establish and Maintain an Enterprise Process for Reporting Incidents

Any employee at Albatross who discovers a security incident must immediately report it to Dick Garfunkel and myself. The reporting will be done via email but a larger organization would probably have a ticketing system in place. Information included in the report would be type of incident, time of discovery, and details of how the incident was discovered. This process would be reviewed annually and the entire control would be available to employees in the company Google Drive.

Control 18: Penetration Testing

Penetration testing is not a necessary security implementation for an IG1 level organization but I would still perform vulnerability scans on the network on a quarterly basis as a limited precaution. A penetration testing program would be an important security control for a larger organization with more moving parts.