CLARK SCHAEFER CONSULTING

Cybersecurity For:

Not-for-Profits

Presented by:

Carly Devlin

Agenda

- Understanding Cyber Risk
- Cyber Threats
- Case Studies
- Managing Cyber Risk
- Cybersecurity Tools
- Questions

Understanding Cyber Risk

CYBER RISK:

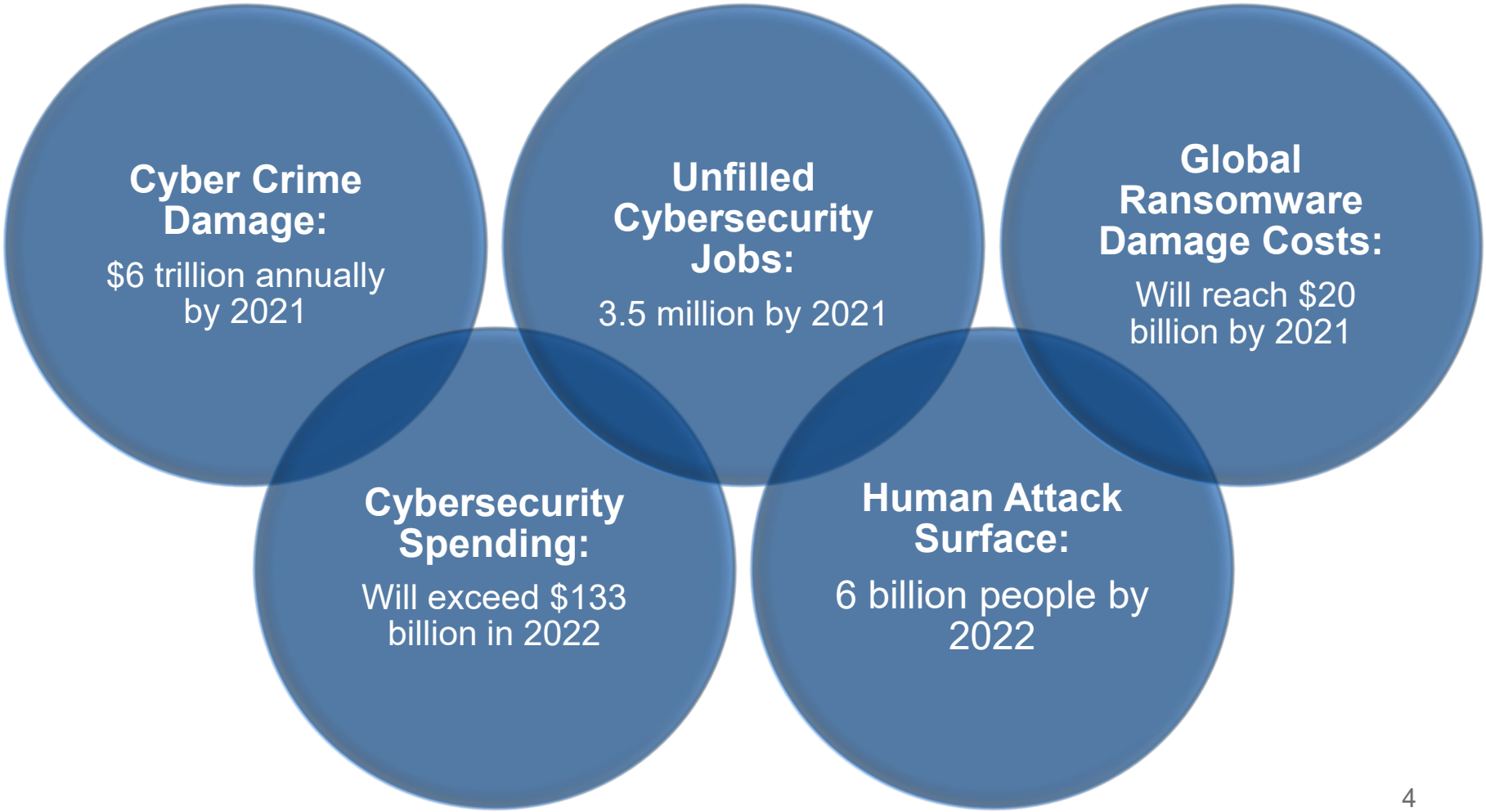
Any risk of financial loss, disruption, or damage to the reputation of an organization from a failure of its information technology systems.

Source: The Institute of Risk Management

FAILURE TO MITIGATE MAY CAUSE:

- System/process disruption
- Loss of confidential data
- Financial loss
- Fraudulent reporting and metrics
- Reputation damage

Cybersecurity Facts



Cyber Threats

Event with the potential to adversely impact an organization, its assets, and/or its individuals through an information system (via unauthorized access, destruction, disclosure, modification of information, and/or denial of service).

Threat Actors	Actor Motives
National Governments	Cyber warfare/espionage
Terrorist Groups	Spread terror
Organized Crime	Financial gain
Hacktivists	Political agenda
Hackers	Notoriety/financial gain
Insider Threats	Revenge/financial gain

2019 Verizon Data Breach Report

2019 Verizon Data Breach Report: Overall Victims

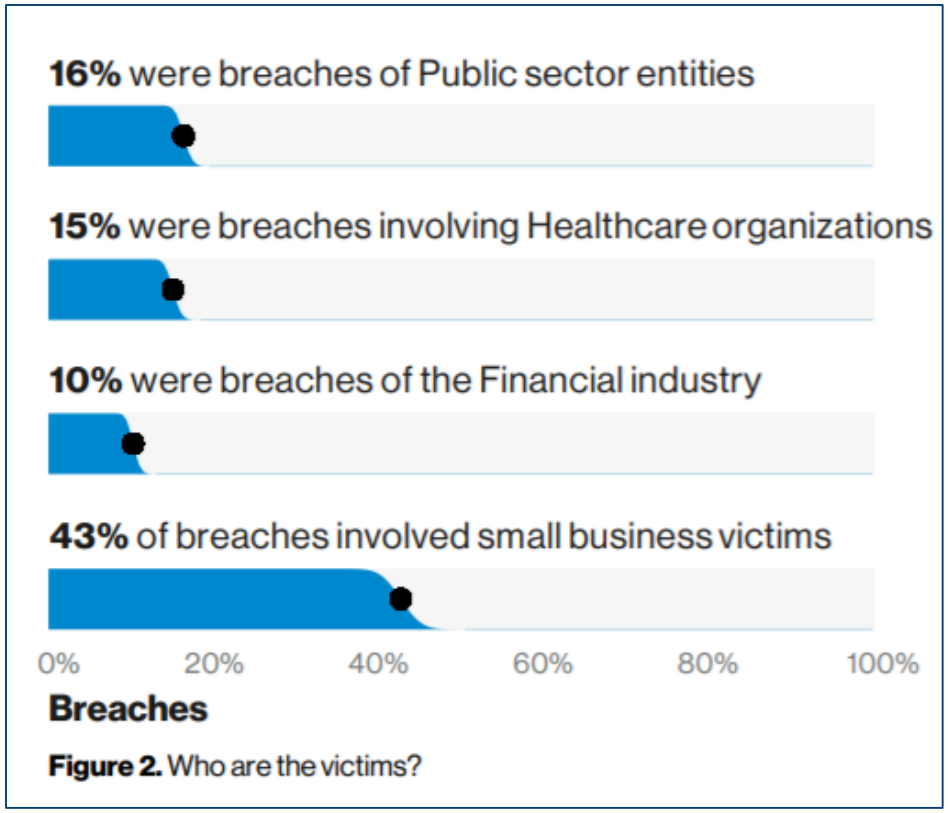


Figure 2. Who are the victims?

State of Nonprofit Cybersecurity Report

- **68%** of nonprofit organizations **don't have documented policies and procedures** in place in case of a cyber attack
- **59%** of nonprofit organizations **don't have cybersecurity training** for staff
- **56%** of nonprofit organizations **don't require multifactor authentication** (MFA) to log into online accounts
- **83%** of nonprofit organizations **have not undergone a cyber attack simulation** activity

Source: NTEN

Our Clients: Most Common Cyber Threats

Phishing

Ransomware

Configuration Errors

Software Vulnerabilities

Internet of Things (IoT)

Case Study #1

Attack Victim	Save the Children
Description	Save the Children was fooled into sending approximately $1 million for solar panels to a project they supported in Pakistan. One worker's email was hacked allowing the hacker to pose as an employee and create fake invoices.

Case Study #2

Attack Victim	The Girl Scouts, Texas Chapter
Description	The organization announced on Facebook that its website had been hacked with the homepage defaced. During the attack, users were registering and paying for camps on the organization's website.

Case Study #3

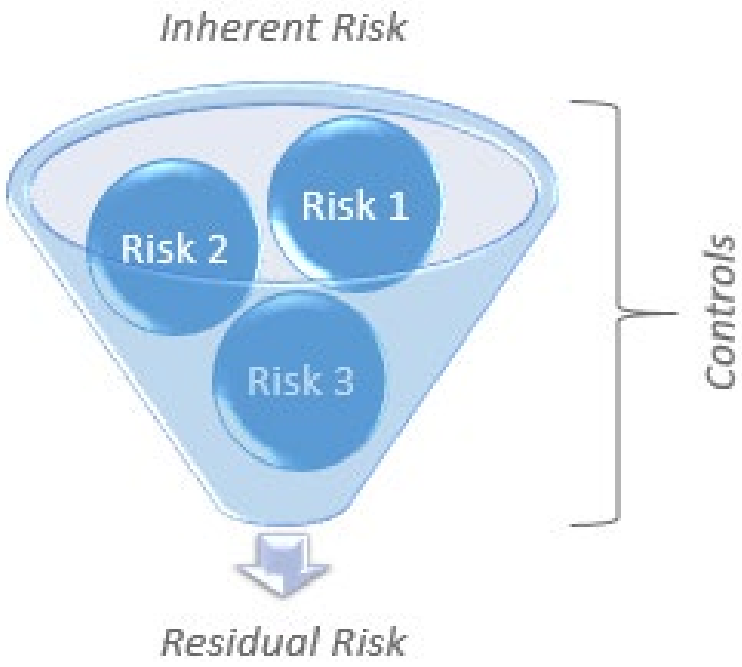
Attack Victim	Utah Food Bank
Description	The organization's website was hacked, and 10,000 visitors who donated online lost their personal information to identity thieves.

Case Study #4

Attack Victim	The Red Barn
Description	The server The Red Barn's website (and others) was located on was attacked and all websites were affected. This occurred during a fundraiser event, so the organization had to remove its website, purchase a new domain name, and rebuild the website from scratch.

Managing Cyber Risk

Mitigation vs. Elimination of Risk



Use of a Security Framework

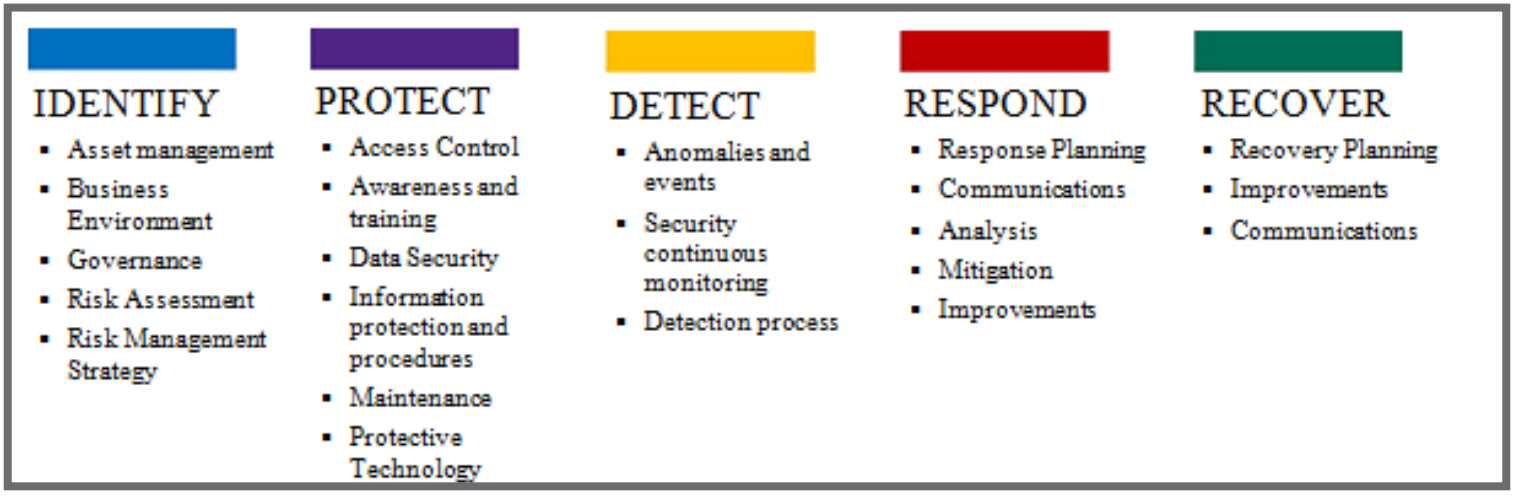
Documented processes used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.

NIST Cybersecurity Framework (CSF)

- **Established by:** The National Institute of Standards and Technology (NIST)
- **Designed to:** Be a US government-ordered, cybersecurity framework
- **Overview:** Provides a common language with which to address and manage cyber risk in a cost-effective way based on business needs, without additional regulatory requirements.

NIST Cybersecurity Framework (CSF)

- **Three Parts:**
  - Framework Core
  - Framework Implementation Tiers
  - Framework Profiles



CSF Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

Applying the CSF

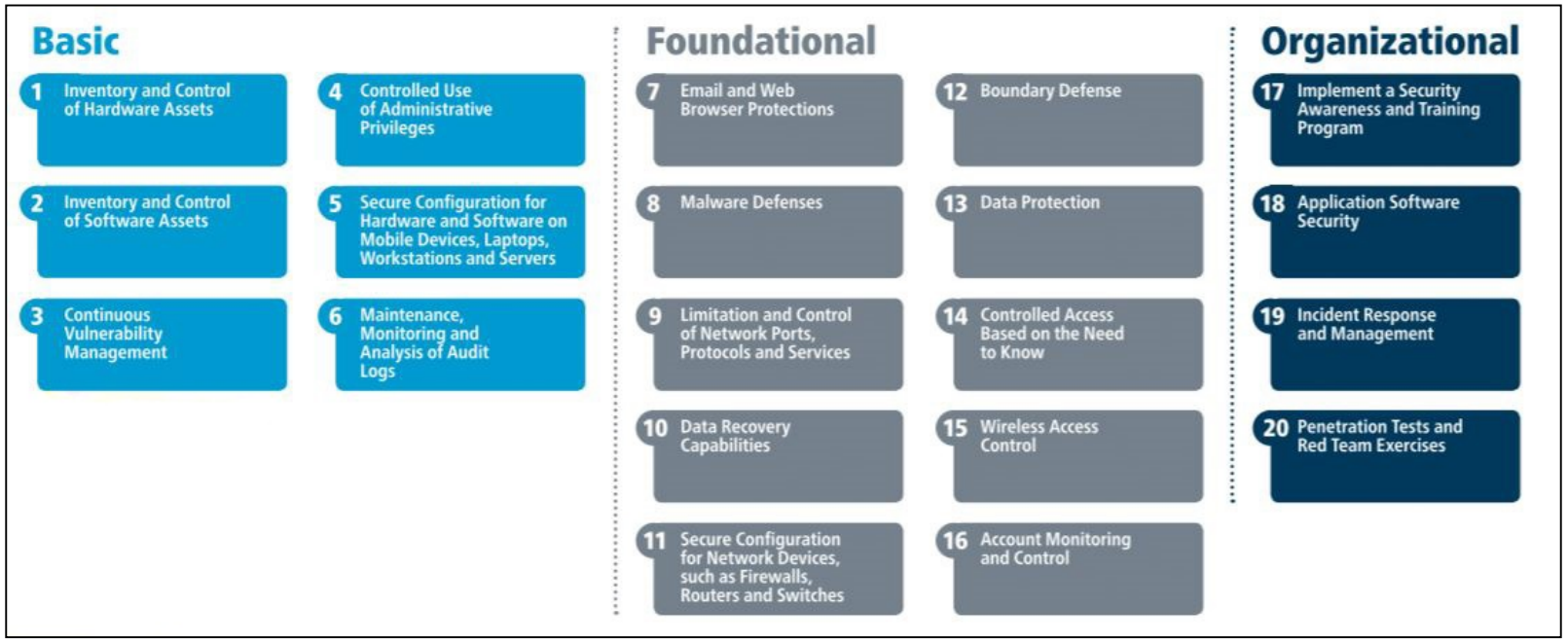
1. Prioritize & scope
2. Orient
3. Create a current profile
4. Conduct a risk assessment
5. Create a target profile
6. Determine, analyze & prioritize gaps
7. Implement action plans

CIS Top 20 Controls Framework

- **Established by:** The Center for Internet Security
- **Designed to:** Be global standards and recognized best practices for securing IT systems and data against the most pervasive attacks
- **Overview:** Can be used to quickly establish the protections providing the highest payoff within organizations. Guides you through a series of foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.

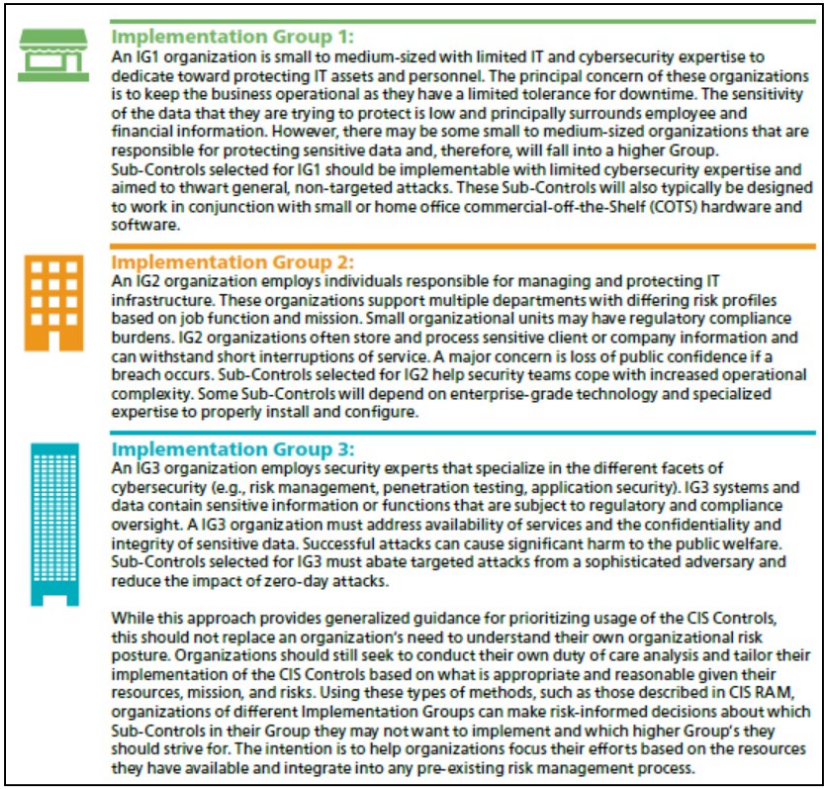
CIS Top 20 Controls Framework

- Implementation helps defeat over 85% of common attacks



CIS Top 20 Implementation Groups

- Implementation groups help determine focus areas depending on type/size of organization



Implementation Group 1:
An IG1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these organizations 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 principally surrounds employee and financial information. However, there may be some small to medium-sized organizations that are responsible for protecting sensitive data and, therefore, will fall into a higher Group.
Sub-Controls selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Sub-Controls will also typically be designed to work in conjunction with small or home office commercial-off-the-Shelf (COTS) hardware and software.

Implementation Group 2:
An IG2 organization employs individuals responsible for managing and protecting IT infrastructure. These organizations support multiple departments with differing risk profiles based on job function and mission. Small organizational units may have regulatory compliance burdens. IG2 organizations often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Sub-Controls selected for IG2 help security teams cope with increased operational complexity. Some Sub-Controls will depend on enterprise-grade technology and specialized expertise to properly install and configure.

Implementation Group 3:
An IG3 organization employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. A IG3 organization must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Sub-Controls selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

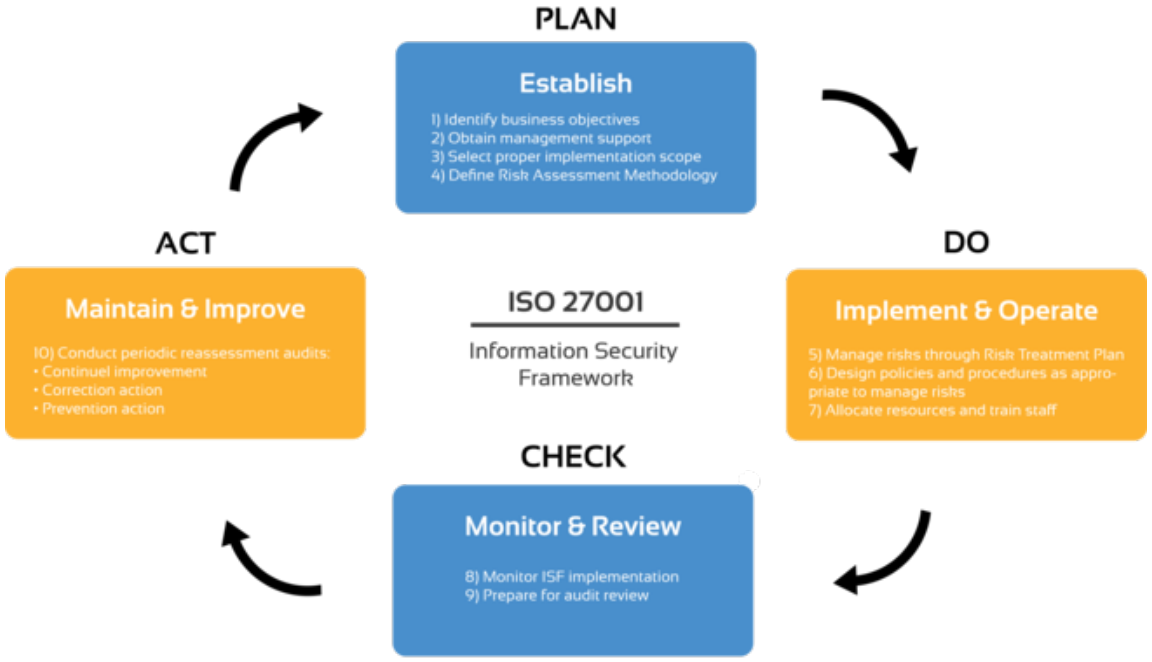
While this approach provides generalized guidance for prioritizing usage of the CIS Controls, this should not replace an organization's need to understand their own organizational risk posture. Organizations should still seek to conduct their own duty of care analysis and tailor their implementation of the CIS Controls based on what is appropriate and reasonable given their resources, mission, and risks. Using these types of methods, such as those described in CIS RAM, organizations of different Implementation Groups can make risk-informed decisions about which Sub-Controls in their Group they may not want to implement and which higher Group's they should strive for. The intention is to help organizations focus their efforts based on the resources they have available and integrate into any pre-existing risk management process.

ISO/IEC 27001

- **Established by:** The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- **Designed to:** Provide requirements for an information security management system (ISMS)
- **Overview:** Requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization

ISO/IEC 27001

- Includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure.



Where to Start?

- Risk Assessment/Audit
- Framework Gap Analysis
- Vulnerability Assessment
- Social Engineering Exercise
- Virtual CISO

CLARK SCHAEFER
CONSULTING

QUESTIONS?

Thank you for your time!

Carly Devlin, CISA, CISSP
Managing Director
614.607.5132
cdevlin@clarkschaefer.com