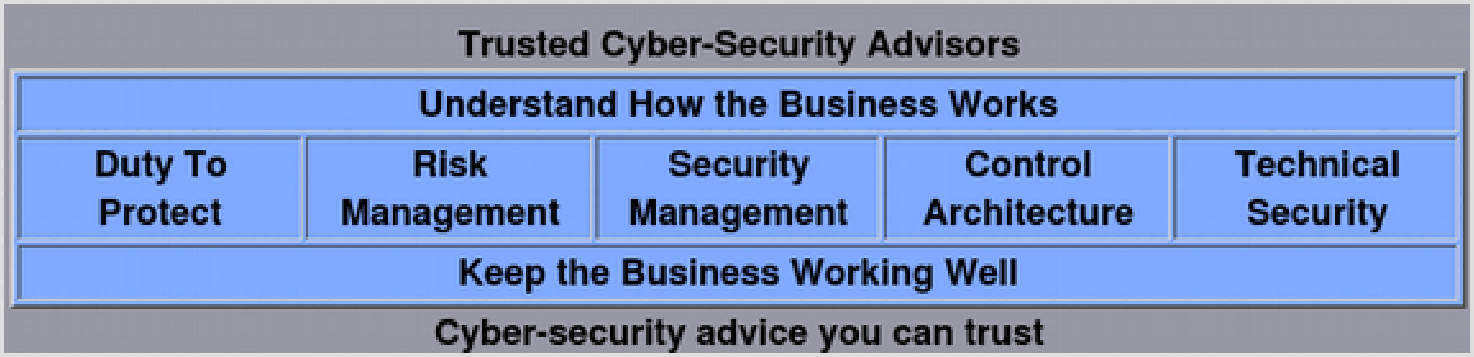
Trusted Cyber

Trusted Advisors Since 1977

Single Point of Contact Document

This is the Single Point of Contact (SPOC) document for our Trusted Cyber-Security Advisory Services offerings. It provides an overview of the services for potential clients and provides pre-onboarding information for our new clients.



Trusted Cyber-Security Advisors

Understand How the Business Works

Duty To Protect | Risk Management | Security Management | Control Architecture | Technical Security

Keep the Business Working Well

Cyber-security advice you can trust

Our service offerings:

We offer two standard service types and augment them on a custom basis as needed:

- **Single Advisor:** This service provides one-on-one advisory services provided by a single advisor in contact with a single point of contact at the enterprise.
  - One-on-one periodic (usually weekly) **live online remote** meetings are used to support the single point of contact at the enterprise.
  - The service is supported by **internal group meetings** and expertise to help augment the single advisory in areas they wish support for.
  - The service uses **internal** use only **tools** to support tracking so **nothing falls through the cracks**, and tools that codify our **standards of practice** to provide for rapid and effective well vetted advice **subject to and augmented by the advisor**'s client knowledge and expertise.
- **Advisory Board:** This service provides an advisory board typically consisting of 4 members:
  - **A lead advisor** who coordinates the service and provides one-on-one assistance in the same way as the single advisor service provides.
  - **An expert from the vertical** who knows the subject matter and understands the industry.
  - **A top manager** who has operated similar sized enterprises in a C-suite position.
  - **A technical expert** who understands the nuts and bolts of the technologies at issue.

Augmented services provide clients with increased intensity efforts as and if needed. This ranges from workshops and pathfinder studies through long-term assistance and temporary corporate executive assistance.

Benefits:

Benefits include:

- Better informed decisions for you and your enterprise
- Documentation of current and future paths across 100+ key decisions as they evolve with time
- Special assistance when you most need it
- Augmentation from trusted experts who already know the issues and context

Please read the rest of this SPOC document carefully to maximize your benefit.

These service offerings are:

- **<u>LIVE</u>** You work in **real-time** with your **advisor** and supporting **content** and **tools**.
- **<u>ONLINE</u>** You do this online using **your computer and the Interne**t.
- **<u>REMOTE</u>** You do it from YOUR location – **no travel** is involved – no wasted resources consumed.

This service consists of:

- **Initial onboarding:**
  - We start with an onboarding process that gives you access to our internal systems.
  - Periodic (weekly, bi-weekly, and/or monthly) meetings are set on a regular recurring basis.
  - Depending on the desire of the client, this is also an opportunity to start providing information within these systems about the current situation and to set up for the future issues identified as important and urgent.
- **Recurring live online remote meetings:**
  - Periodic meetings provide regular contact where we:
    - Act on urgent issues
    - Provide additional information per requests in the interim
    - Work through a wide range of long-term strategic decisions
    - Develop plans and calendar activities for future meetings
- **Follow-on:**
  - Periodic meetings produce follow-ons performed between meetings
    - Some are simple content identification and provisioning
    - Some involve group discussions among our advisory group
    - Some are more complex longer-term efforts requiring augmentation to normal services
- **Urgent care:**
  - Between regular meetings, urgent issues can produce urgent care contacts
    - Urgent matters are usually responded to within 24 hours with immediate advice
    - If more in-depth assistance is required, augmented services may be provisioned
    - Urgent care calls may also be made with advisory board members (for those with boards)
- **Augmentation:**
  - Clients identify:
    - Special needs that we are well suited to meet quickly and efficiently.
    - Urgent needs for assistance between regular meetings.
    - Larger projects advisors can assist in.
  - Using the in-depth information from our existing relationship, we service these needs for additional fees.
  - We try to act within your direct decision-making power, and without the need for additional contracts or processes that can delay service or hinder outcomes.

Standard coverage areas

In addition to our standard coverage areas (listed here), we also cover special topics particular to each entity. The following standard coverage areas are supported when other priorities don't override them:

- **Overarching: How does the enterprise describe itself and why this effort is being undertaken?**
- **Overarching: Protection model: What model is used to understand information protection issues?**
- **Overarching: Business: What is the nature of the business?**
- **Overarching: Promises: What promises does the business make, to whom, and why? How do they relate to information?**
- **Overarching: Scope: What is the scope of this security architecture?**
- **Overarching: Maturity level: What maturity level does the information protection program have?**
- **Overarching: Location: Where are content and work located?**
- **Overarching: Organization: What is the structure of the organization?**
- **Overarching: Security consultants: When are information security consultants used?**
- **Overarching: Mobility: What part and portion of the workforce is mobile?**
- **Overarching: Outsourcing people: What part and portion of the workforce is outsourced?**
- **Overarching: Outsourcing things: When is information technology outsourced?**
- **Risk Management: Risk definition: How are risk levels for the protection program defined?**
- **Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?**
- **Business modeling: How does the enterprise model itself and its business?**
- **Business modeling: What are the business functions and what information do they depend on for what?**
- **Oversight: What does enterprise oversight provide to the protection program to define duties to protect?**
- **Oversight: How are different sorts of duties prioritized in determining what to protect and how well?**
- **Oversight: Form of duties: What form are duties defined in?**
- **Oversight: Duties analysis: How is duty to protect analyzed?**
- **Risk Management: How does the enterprise do risk management?**
- **Risk Management: Risk management process: What risk assessment processes are used?**
- **Risk Management: Threats: How are information-related threats assessed?**
- **Risk Management: Threats: What threats have been identified, what are their characteristics and relevant history?**
- **Risk Management: Threats: What design basis threat is used?**
- **Risk Management: Threats: What attack mechanisms are considered?**
- **Risk Management: Vulnerabilities: How and when are information-related vulnerabilities assessed?**
- **Risk Management: Risks: When does the enterprise avoid, accept, transfer, and mitigate information-related risks?**
- **Risk Management: Risk aggregation: What process is used to identify and control the aggregation of risks?**
- **Risk Management: Separation of Duties: How should duties be separated?**
- **Risk Management: Interdependencies: How are supply chain risks managed?**
- **Risk Management: Interdependencies: How are real-time interdependency risks managed?**
- **Risk Management: Costs: How is security budgeted?**
- **Risk Management: Surety matching: How is surety matched with risk?**
- **Risk Management: Failsafes: When failsafes are required and how are they determined?**
- **Risk Management: Changing systemic risks: How is changing systemic risks managed?**
- **Risk Management: Changing subsystem risk and surety: How are risk and surety changes of a subsystem handled?**
- **Management: How does the enterprise manage the information protection program?**
- **Management: CISO: Is there an enterprise information protection (IP) Lead, and where are they placed?**
- **Management: Duties: What duties does the information IP Lead have?**
- **Management: Influence: What power and influence does the IP Lead have?**
- **Management: Security Metrics: What security measurements are taken and when?**
- **Management: Policy: What information security policies are needed and used?**
- **Management: Standards: Which widely used control standards are best suited to the enterprise?**
- **Management: Procedures: What procedures are implemented and how?**
- **Management: Documentation: How are security-related issues documented?**
- **Management: Auditing: How are audits managed within information protection?**
- **Management: Intelligence operations: What intelligence (and counter-intelligence) operations are in place?**
- **Management: Testing: What does the testing function do and cover?**
- **Management: Personnel: How are personnel issues with information protection managed?**
- **Management: Background checks: When are which background checks done on which workers?**
- **Management: Incident handling: How are incidents managed?**
- **Management: Legal issues: How do legal issues interact with protection management?**
- **Management: Physical security: How is physical security integrated with information protection?**
- **Management: Knowledge: How is the knowledge program integrated with information protection?**
- **Management: Security awareness: What sort of enterprise security awareness program does the enterprise have?**
- **Management: Exceptions: How are exceptions to normal operational requirements managed?**

Standard coverage areas (cont)

The following standard coverage areas … continued:

- **Control Architecture: How does the enterprise model information-related controls?**
- **Control Architecture: Establishment: Is a control architecture formally established?**
- **Control Architecture: Objectives: What are the protection objectives and how are they applied??**
- **Control Architecture: Access Controls: What access control model is used?**
- **Control Architecture: Identification: How are individuals originally identified and their identities verified?**
- **Control Architecture: Identity proofing: How are asserted identities proofed after originally identified?**
- **Control Architecture: Authentication: How are identities authenticated to support authorized access?**
- **Control Architecture: Access facilitation: How is access facilitated once identity is adequately established?**
- **Control Architecture: Trust model: How is trust assessed and managed?**
- **Control Architecture: Change management: How are changes to information technology managed?**
- **Control Architecture: Control Architecture: When is a systematic security architecture created and updated?**
- **Technical Security Architecture: How are technical controls structured?**
- **TechArch: Inventory: What information protection-related inventory is kept and in what form(s)?**
- **TechArch: Workflows: How are workflows used, controlled, and assured?**
- **TechArch: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?**
- **Zones: How does the enterprise separate parts (zone) its network(s)?**
- **Zones: Placement: What systems, data, and people go in which zones and subzones?**
- **Zones: Firewalls: What mechanisms are used to separate communicating zones and subzones?**
- **Zones: Zone separation verification: How is zone separation verified?**
- **Zones: Physical separation: How are zones and subzones physically separated and controlled?**
- **Zones: Connection controls: How are connections between devices controlled?**
- **Zones: Microzones: How is virtualization and encryption used to for microzones and when?**
- **Zones: Remote access: How is access to internal zones from distant locations (including wireless) facilitated?**
- **Zones: Endpoint protection: What protective mechanisms are used to harden which endpoints?**
- **Zones: Zone to zone access: How is communication facilitated and controlled to areas outside a zone/subzone?**
- **Incidents: Detection: Are intrusions detected, and if so, how?**
- **Incidents: Malicious Alteration Detection: How is malicious alteration detected?**
- **Incidents: Response: Who controls and executes responses to information-related attacks?**
- **Incidents: Detection and response: What are the process requirements for detection and response?**
- **Incidents: Deception: When are deceptions used to defend networks and systems?**
- **Content control: How is harmful and useless content controlled in my computing environments?**
- **Content control: What mechanisms keep control over content with business utility?**
- **Content control: Data in use: How is data in use protected?**
- **Content control: Data in motion: When is content in transit encrypted?**
- **Content control: Data at rest: What is stored encrypted?**
- **Content control: Version control: How are versions of data over time protected?**
- **Content control: How is intelligence gathering countered?**
- **Content control: How is intellectual property protected?**
- **Human factors: How are human factors considered in the protection program?**
- **Human factors: Protection load: How is security load managed?**
- **Human factors: User real-time decision-making: What is considered in real-time human decision-making?**
- **Human factors: Real-time decision-making methodology: How are real-time decisions structured?**
- **Human factors: Disruption: How is disruption of work controlled?**
- **Redundancy: Fault model: What fault model is assumed for analysis of redundancy?**
- **Redundancy: Backups: What is backed up and how often?**
- **Redundancy: Backup retention: How long are backups retained and how are they disposed of?**
- **Redundancy: Storage location: Where and in what sort of containers are backups stored?**
- **Redundancy: Data center redundancy: How many data centers are required?**
- **Redundancy: Redundant facility distance: How far apart are redundant data centers and people to assure continuity?**
- **Redundancy: Business continuity and disaster recovery: What information resources are where?**
- **Redundancy: Interdependencies: How is redundancy applied to interdependent mechanisms?**
- **Technology: Logical Perimeters: What logical perimeters have what protection mechanisms?**
- **Technology: Physical Perimeters: What physical perimeters have what protection mechanisms?**
- **Technology: Physical/Logical Nexus: How do physical and logical controls interact and integrate?**

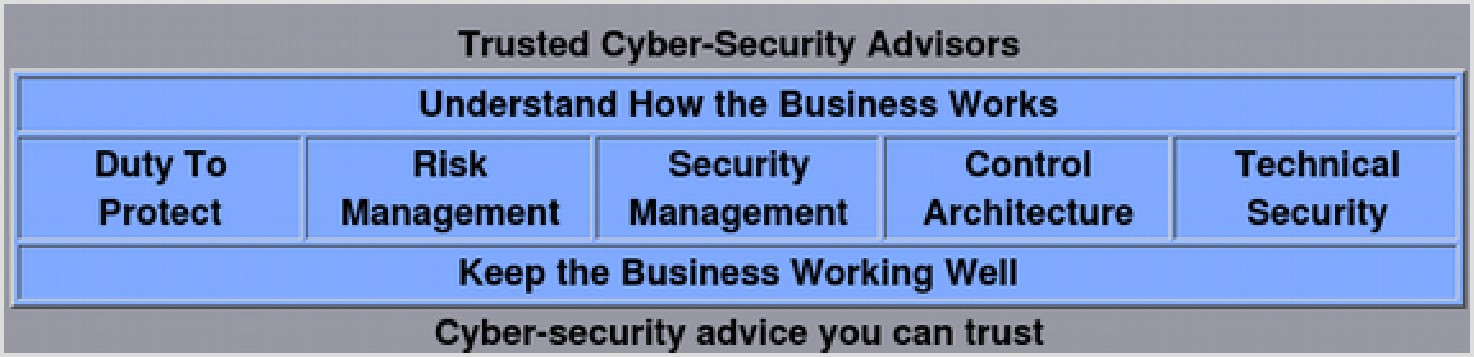
Checklist

Please use this checklist to facilitate your efforts to succeed through the process.

What	Done?
Setup your recurring payments and make the initial payment	
Reply to the invitation email after you pay	
Set a date and time for onboarding with our team and your (lead) advisor	
Receive and confirm the meeting invitation scheduling your onboarding meeting	
Make certain the meeting is in your calendar and that you reserve enough time for the meeting	
Test out zoom.us and make sure it works on your system(s)	
Identify periodic days of week and times of day you can make regular meetings	
Attend the onboarding session • We will provide access credentials during that meeting • You will need to be able to use your Web browser to access distant sites • You will gain access to content and systems used in the services • You will be briefly trained on the use of those systems • We will schedule the periodic meetings • We will send and you will receive and confirm calendar invitations for these meetings • You will get contact details for urgent communications in case needed • You will be able to ask any questions you have • Based on the process desired, you will be given “homework”	
Perform the “homework” associated with the first meeting in advance	
Be on the first meeting ready to go	

Checklist for Advisory Services Onboarding Process

Summary:



Trusted Cyber-Security Advisors

Understand How the Business Works

Duty To Protect

Risk Management

Security Management

Control Architecture

Technical Security

Keep the Business Working Well

Cyber-security advice you can trust

Let us know about any questions regarding our coverage, processes, people, approach, or anything else you want to know. Welcome to our services, and we hope to start working with you soon.