IT Security Governance Council Charter

I. Purpose

The IT Security Governance Council (ITSGC) is established to support and enhance the security posture of the organization by ensuring adherence to IS-3 policy, facilitating effective security practices, and promoting a culture of security awareness and responsibility.

II. Responsibilities

A. Support IS-3 Policy

- Uphold and promote the principles and practices outlined in the IS-3 policy.
- Ensure organizational alignment with IS-3 policy requirements and objectives.

B. Assist CISO in Selecting:

- Information Security Industry Standards:
  - Provide justifications based on current industry standards and input from the Information Security team.
  - Evaluate and recommend CISO-approved encryption methods and standard exceptions, ensuring they are justified and supported by appropriate mitigations.
- Network Protection Technologies:
  - Provide justifications aligned with current industry standards.
  - Ensure network configurations are justified and adhere to the prevailing industry standards.
- Data Transfer Technologies:
  - Provide justifications in line with current industry standards.

  - Ensure technologies employed are in accordance with Appendix DS accepted CISO-approved equivalents.

C. Periodic Review and Justification:

- Local and System-wide Policies:
  - Evaluate the relevance and effectiveness of existing policies.
  - Recommend updates or enhancements to align with evolving security landscapes.
- Standards and Procedures:
  - Assess the applicability and adequacy of standards and procedures.
  - Propose modifications to enhance security measures.
- Roles and Responsibilities:
  - Review the roles of Unit Heads, UISLs, UIRLs, CISO/Deputy CISO, and CRE to ensure clarity and effectiveness.
  - Recommend role enhancements or modifications to optimize security governance.
- Security Exceptions and Compliance:
  - Review open/active security exceptions for P3 or higher IT resources.
  - Assess the current state of compliance of P3 or higher IT resources.
- Technology and Configuration:
  - Evaluate network protection technologies, network configurations, and data transfer technologies.
  - Ensure alignment with industry standards and organizational requirements.
- Supplier Risk Assessment:
  - Review and make recommendations for the supplier risk assessment process & tool to ensure appropriate risk-based security evaluations.

D. Audit Reviews and Recommendations:

- IS-3 Compliance at UC Santa Cruz:
  - Review audits of IS-3 compliance.
  - Track and make recommendations for enhancements.
- IS-12 Compliance at UC Santa Cruz
  - Review audits of IS-12 compliance
  - Track and make recommendations for enhancements.
- Marsh Cybersecurity Self-Assessment Results:
  - Evaluate the results and propose action plans for improvement.
- SHS HIPAA Assessments Results:
  - Review assessments and recommend strategies to address identified gaps.

III. Membership

The council will consist of representatives from various units, including but not limited to IT, audit/compliance, legal, privacy, risk services, financial services, office of research, health services, and the campus police department. The CISO will provide oversight, and Unit heads may delegate this role within their organization.

- Chief Information Security Officer
- Audit
- Privacy
- Police Dept.
- Legal
- Registrar's office
- University Relations
- Risk services
- Financial affairs
- Faculty
- Student representative

IV. Meetings

The council will meet twice per year or as needed to address emerging issues. Special meetings with SMEs can be convened at the request of the CISO or a majority of council members.

V. Reporting

The council will report its findings, recommendations, and action plans to the campus leadership team on a quarterly basis or as needed to address urgent issues.

VI. Review and Amendments

This charter will be reviewed annually by the council and amended as necessary to meet the evolving needs of the organization’s IT security posture.

Previous notes

- Support IS-3 policy
- Assist CISO in selecting
    - Information Security Industry Standard
        - Justification
    - CISO-approved encryption method

        - Input from Information Security team
        - Current industry standard
    - CISO-approved standard exceptions
        - Justification
        - Mitigations
    - Network protection technologies
        - Justification
        - Current industry standards
    - Network configuration
        - Justification
        - Current industry standard
    - Data transfer technologies
        - Justification
        - Current industry standard
    - Appendix DS accepted CISO-approved equivalents
- Periodic review of, and justification for
    - Local policies
    - System-wide policies
    - Standards
    - Procedures
    - Unit Heads and UISLs
    - CISO and CRE roles
    - CISO-approved encryption method
    - Open/active security exceptions for P3 or higher IT resources
    - P3 or higher IT resources and their current state of compliance
    - Network protection technologies
    - Network configuration
    - Data transfer technologies
    - Supplier risk assessment process & tool
- Review audits of, track and make recommendations on MCAs
    - IS-3 compliance at UCSC
    - Marsh cybersecurity self-assessment results
    - SHS HIPAA assessments results