Segal's 15th Annual Multiemployer IT Summit

October 6, 2021

Segal

Introduction
Information Security Governance

Establishing and Maintaining an Information Security Governance Committee (ISGC) for Trusts

Michael Stoyanovich
VP and Senior Consultant, Segal

Introduction

Today's Summit and Future Conferences

Feedback Opportunities

- Real-time polling
- Real-time breakout sessions
- Near-time Q&A
- Survey

Consider What Topics are Most Important to Your Organization

- Now
- Next month
- In 6 months
- Next year

Panel Discussion

Innovation and Automation During and After COVID-19

Polling Question 1

What are the key challenges you are facing in returning to the office?

1. Staffing shortage (Hiring and retaining employees)
2. COVID policies to return to the office
3. Automating work processes
4. Implementing self-service processes
5. Data security

Information Security Governance

Establishing and Maintaining an Information Security Governance Committee (ISGC) for Trusts

Information Security Governance Committees can help Trusts understand and mitigate risks to Trust and participant data and information.

DOL Weighs in with Best Practices and Tips

- **April 2021** — first official DOL guidance
- Emphasized that fiduciaries must ensure proper mitigation of security risk, DOL clarified the need to evaluate, select, and contract with service providers that take steps to minimize security risk - and monitor service providers to ensure compliance with contract terms
- Follows cybersecurity-related retirement plan litigation involving plan sponsors, service providers

Three Components of the Guidance Include:

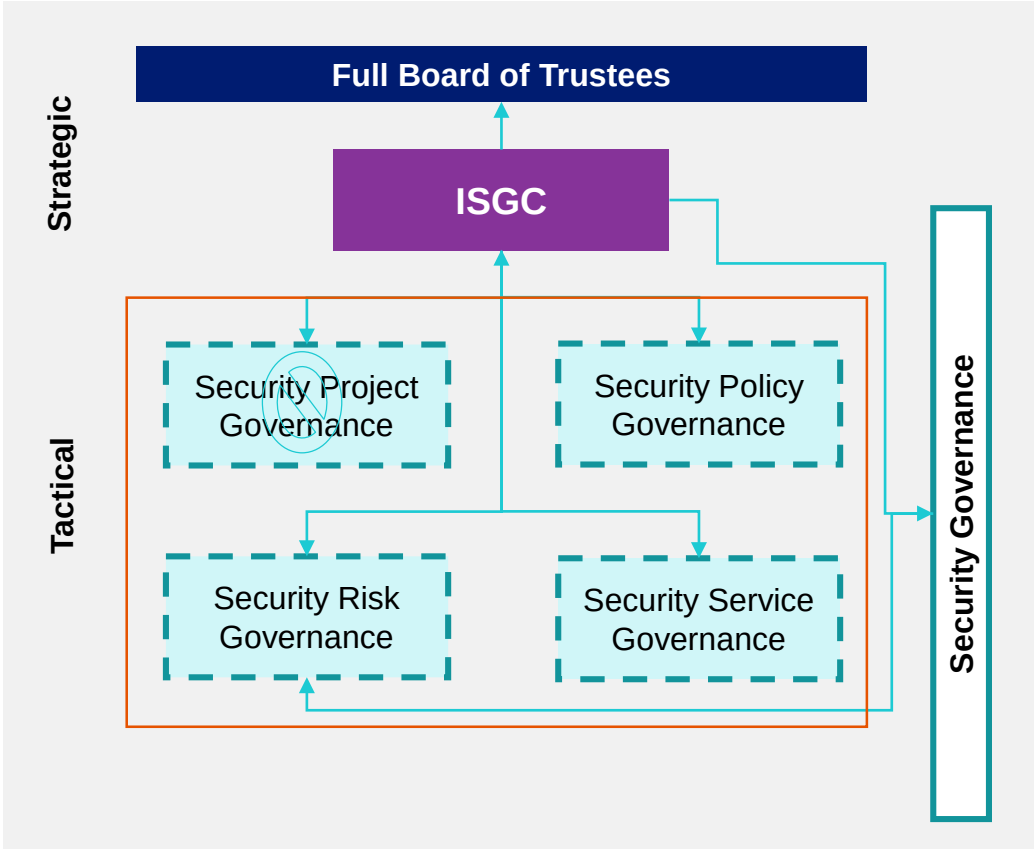
1. Cybersecurity Program Best Practices
2. Tips for Hiring a Service Provider with Strong Cybersecurity Practices
3. Online Security Tips

Segal's ISGC Trust Process

1. Establish the Committee

Establish High-level ISGC Processes to Enable Committee Functionality

- A successful committee requires clarity over responsibilities between the Trust, vendors and trading partners.
- Stratifying processes based on domains clarifies
  - The definition of roles and accountabilities
  - Helps partition activities based on organizational areas so actions can be taken to satisfy governance requirements
- Understanding information flows is important.



Establish High-level ISGC Processes to Enable Committee Functionality

- ISGC is a subset of Trustees and Fund Counsel
- A common mistake: Trusts build their committee charters and launch into their first meeting without defined inputs and outputs
- What happens when this occurs? The committee:
  - Does not have the needed information to execute on responsibilities
  - Is unable to meet its stated goals
- Building high-level processes defines how information flows within and between committees and enables rapid decision making
- Participants have information they need to be confident in their decisions

Potential Information Security Governance Committee (ISGC) Responsibilities and Duties

Strategic Oversight

- **Provide oversight and ensure alignment** between information security requirements of the Trust and its participants and the vendors / trading partners servicing the Trust and its participants
- **Assess adequacy of resources** to sustain and advance successful security programs and practices for identifying, assessing, and mitigating information security risks across all vendors / trading partners

Policy Governance

- **Review vendor / trading partner policies** pertaining to information security and cyberthreats, taking into account the potential for external threats, internal threats, and threats arising from transactions with their own trusted third parties and other vendors (vendors who serve the Trust's vendors)

Potential Information Security Governance Committee (ISGC) Responsibilities and Duties

Strategic Oversight

- **Review vendor / trading partner controls** to prevent, detect, and respond to cyber-attacks or information or data breaches involving Trust and participant electronic information, intellectual property, data and information.
- **Review vendor and trading partner cyber insurance policies** to ensure appropriate coverage.

Policy Governance

- **Review privacy and information security policies and standards** and the ramifications of updates to policies and standards.

Define ISGC Meeting Agendas and Procedures

Review responsibilities, participants, and timing of meetings and ongoing reporting

- **Annual Meeting:** Identify if all responsibilities that will be included in annual meeting (likely all governance responsibilities expected for the upcoming year)
- **Quarterly Meeting:** List of responsibilities for quarterly meetings.
- **Monthly Reporting**: Dashboards and other reports to the ISGC produced reporting on the status of survey responses and associated disposition of those responses (risk is ‘high’, ‘medium’, or ‘low’).

Input

- Responsibility cadence

Output

- ISGC annual, quarterly meeting agendas & procedures

Materials

- ISGC Charter

Participants

- ISGC committee members and associated professionals.

Define Which Vendors and Metrics ISGC Will Survey and Monitor

1. Consider your Trust's specific ISGC purpose and responsibilities (e.g., govern the use of health data, pension data, financial data, etc.)
2. For each domain, identify which vendors and associated metrics you wish to survey
3. Monitor and determine whether these are valuable to the Trust, to Trustees, to participants, or all stakeholders
4. Decide to monitor them, an ongoing basis — or not

Input

- List of vendors and associated metrics to survey and monitor.

Output

- Metrics, by vendor or trading partner to report to the Governance Committee.

Define Which Vendors and Metrics ISGC Will Survey and Monitor

Possible Metrics

1. Review example metrics on the following slides
2. Determine potential alignment with your purpose and responsibilities sections of the charter
   - Trustee and legal counsel suggestions are welcome
3. Finalize list of metrics to survey
4. Track those that cover the major areas of your charter responsibilities

Input

- List of vendors and associated metrics to survey and monitor.

Output

- Metrics, by vendor or trading partner to report to the Governance Committee.

Potential Information Security Governance Committee (ISGC) Responsibilities and Duties

Risk Governance

- **Review and approve** vendor / trading partner information security risk governance structure and key risk management processes and capabilities
- **Assess vendor / trading partner's security** of Trust or participant related information assets and **highlight gaps** and/or call attention of the ISGC to information privacy and security needs based on survey response.

Monitoring & Reporting

- **Receive and review periodic reports** from vendors / trading partners and coordinate with Trustees on metrics used to measure, monitor, and manage information security risks posed to the Trust and its participants by these vendors / trading partners

Potential Information Security Governance Committee (ISGC) Responsibilities and Duties

Risk Governance

- **Review the vendor / trading partner's cyber-response** preparedness, incident response plans, and disaster recovery capabilities as applicable to the vendor /trading partner's information security strategy based on survey responses.
- **Provide input to Trustees** regarding the vendor / trading partner's information risk profile pertaining to Trust or participant data and information.

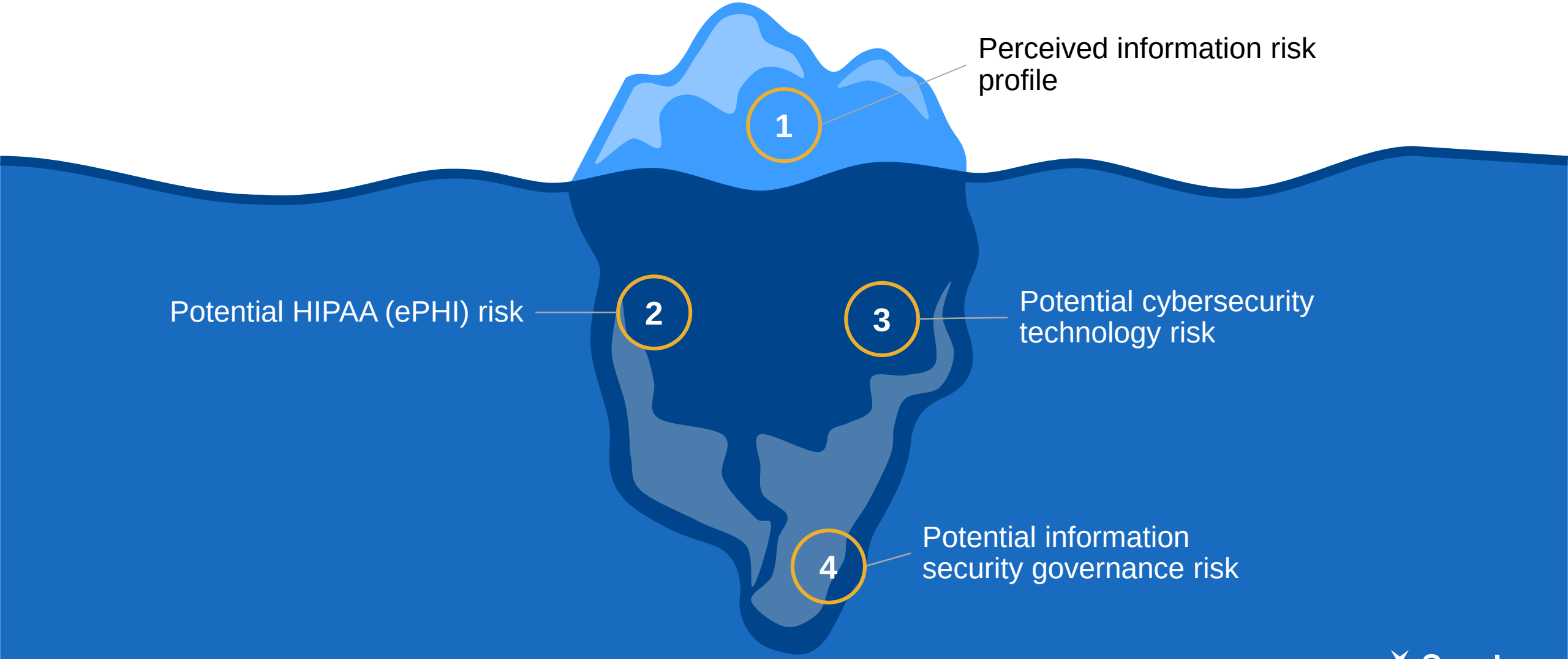
Monitoring & Reporting

- **Assess the quality and effectiveness** of the vendor / trading partner's technology security, capabilities for disaster recovery, data protection, cyber threat detection and cyber incident response, and management of technology-related compliance risks based on survey information reported to Segal.
- **Share reports** (dashboard, etc.) on a monthly basis with the ISGC.

2. Survey Vendors & Trading Partners

3. Monitor

Survey and Then Assess Vendors and Trading Partners for Potential Risks to the Trust and Participants



Potential Metrics on Which to Survey Vendors And then Monitor, Ongoing

Type	Name	Description
Document Request & Review	Security Policies	Vendor security policies should be assessed for completeness, communication, and recency
Document Request & Review	Security Architecture	If vendor has developed a security architecture, this should be reviewed for completeness
Document Request & Review	Security Control Framework	If vendor has adopted a security control framework, this should be reviewed for alignment with industry standards
Document Request & Review	Security Strategy	If vendor has a security strategy, this should be reviewed for completeness and recency
Document Request & Review	Security Certifications (e.g. ISO 27001, PCI)	If vendor has any security certifications, these should be reviewed for applicability
Document Request & Review	Security Audit Reports	Internet or external security audit reports should be reviewed for any outstanding findings or omissions
Document Request & Review	Most Recent Vulnerability Assessment Report	Review vulnerability assessment reports for applicability and for any outstanding critical findings
Document Request & Review	Most Recent Penetration Test Report	Review penetration test reports for applicability and for any outstanding critical findings
Document Request & Review	Security Incident Management Plan	Review security incident management plans for completeness and recency
Document Request & Review	Security Incidents	Review security incident logs for evidence of lessons learned – these may also be used for compromise diagnostics
Document Request & Review	Security Metrics	If the vendor has developed security metrics, review for potential issues with security controls.

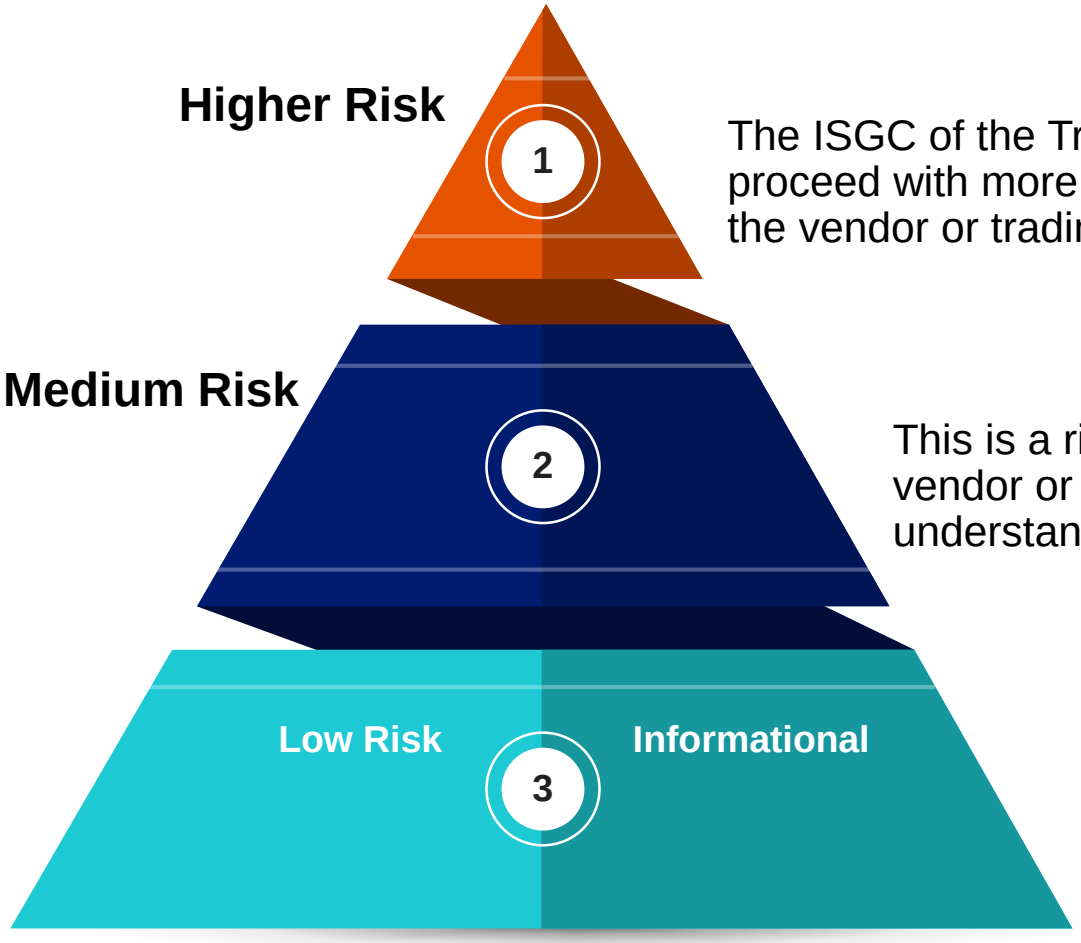
Potential Metrics on Which to Survey Vendors And then Monitor, Ongoing

Type	Name	Description
Document Request & Review	Security Risk Assessments	Review any recent internal or external threat or risk assessments for outstanding finding
Document Request & Review	Compliance Obligations and Reports	Review the list of security compliance obligations and associated compliance reports, for compliance risks – this include HIPAA assessments, SSAE 18, et
Document Request & Review	Security Services / Processes	Review list of security services or processes for completeness
Document Request & Review	Security Systems	Review list of security tools for completeness
Document Request & Review	Security Organizational Structure	Review vendor security organizational structure for completeness
Document Request & Review	Risk Register	If the vendor has a security risk register, review for any unmitigated risks above risk tolerance
Document Request & Review	Security Awareness Program	Review retails related to the vendor security awareness program for completeness and relevance

Present Initial Survey Findings and Ongoing Assessments In A Simple, Brief Format

Identify high, medium and low risk items for the ISGC of the Trust, by vendor or trading partner and report on dashboards and reports

If a higher risk is identified and Fund Counsel agrees, Trustees are potentially obligated to pursue assurance actions, seeking more data and information from the vendor or service provider



The ISGC of the Trust should potentially proceed with more and closer inspection of the vendor or trading partner.

This is a risk or risks to follow up with the vendor or trading partner about; gain better understanding of their perspective.

For Higher Risks, the Trust May Seek Help to Oversee Assurance Action on Behalf of the ISGC

Type	Name	Description
Assurance Action	Engage Third Party Security Assessment	In some situations, engage a third party to conduct a security assessment of the vendor
Assurance Action	Request Cyber Risk Rating	In some situations, acquire a Cyber Risk Rating for the vendor and reviewed for any critical findings
Assurance Action	Conduct Vulnerability Assessment	In some situations conduct a vulnerability assessment against the vendor
Assurance Action	Conduct Penetration Test	In some situations, conduct a penetration test against the vendor
Assurance Action	Conduct Interviews	In some situations, interview key security personnel to obtain better insight into risks and compromise diagnostics
Assurance Action	Conduct Public Data Breach Search	In some situations, search public data breach information sources to determine if vendor had a recent security breach
Compromise Diagnostic	Assess compromise diagnostics	In some situations, assess current state of detection controls at the vendor as part of compromise diagnostics
Compromise Diagnostic	Deploy compromise diagnostics	In some situations, if the detection controls at the vendor are deemed inadequate, it may be necessary to deploy new detection controls

Thank You!