



# Sustainability Reporting and Internal Controls IT's Role, Value and Opportunities

Presented by  
Douglas Hileman, FSA, CRMA, CPEA  
Douglas Hileman Consulting LLC  
at  
ISACA Minnesota Chapter  
July 25, 2024



©2024 Douglas Hileman Consulting, LLC

1

---

---

---

---

---

---

---

---



## Objectives & Agenda

### Objectives

- Gain more understanding of Sustainability Reporting: frameworks, requirements, risks
- Envision roles where IT function can provide support, add value

### Agenda

- 1) Sustainability – “Compliance”
- 2) Sustainability Reporting Standards, Frameworks
- 3) COSO & Internal Controls over Sustainability Reporting
- 4) Tips for the IT / IT Security Functions

7/25/2024

©2024 Douglas Hileman Consulting, LLC

2

2

---

---

---

---

---

---

---

---



## Disclaimer



Presenter provides no warranty, express or implied.

Neither this slide deck, nor the session create a consulting relationship. The opinions are those of the presenter only, and not of any client, organization, or entity affiliated with the presenter.

The presenter is not a CPA.



7/25/2024

©2024 Douglas Hileman Consulting, LLC

3

3

---

---

---

---

---

---

---

---



# 1 Sustainability Compliance: Channels

- Legal and regulatory
  - Enforceable by sovereign entity
  - Legal/ contractual
  - Enforceable by business partner
- Industry standards, frameworks, codes of conduct
- Voluntary obligations



7/20/2024

©2024 Douglas Hillman Consulting, LLC

4

4

---

---

---

---

---

---

---

---

---

---



## Sustainability Compliance: Legal/ Regulatory

### Traditional

- EPA, OSHA
- Department of Labor (wages, equal opportunity)
- Consumer Product Safety Commission
- Federal Trade Commission (Green Guides)

### More Recent

- SEC Conflict Minerals
- California: Consumer Privacy Act, Transparency in Supply Chains Act
- Cybersecurity
- Plastic bag bans
- UK Modern Slavery Act (2015)

7/20/2024

(c) 2024 Douglas Hillman Consulting LLC

5

5

---

---

---

---

---

---

---

---

---

---



## Sustainability Compliance: Legal/Regulatory: **Newer/Emerging**

### Newer/ Emerging

- SEC
  - Guidelines for climate (2010); proposed rule (2022); **final rule (3/6/2024)**
  - Guidelines for human capital disclosures; more coming?
- Inflation Reduction Act, CHIPS and Science Act
- Uyghur Forced Labor Protection Act
  - U.S. Customs and Border Protection Agency
- California SB 253\*, SB 261, AB 1435 (climate; \* = assurance req'd.)
- German Due Diligence Act

Why should U.S. companies be concerned with laws passed elsewhere?

7/20/2024

©2024 Douglas Hillman Consulting, LLC

6

6

---

---

---

---

---

---

---

---

---

---



## Sustainability Compliance: Legal/Regulatory: About IFRS



- DH Views**
- Capital markets are "driving the bus."
  - SASB built disclosure standards on U.S. Supreme Court definition of "materiality"; no new law or regulation was required. [SASB now part of IFRS.]
  - Whatever SEC does (or does not) do, the trend globally is towards more Sustainability disclosures in financial filings.
  - There are general standards. And climate standards. Next up?: Wait and see.
  - Disclosures include data and information along supply chain/ value chain.
  - If you source outside US, or if you sell outside the US, some aspects of these will apply to you.

Why should U.S. companies be concerned with laws passed elsewhere?

7/25/2024

©2024 Douglas Wilson Consulting, LLC

7

---

---

---

---

---

---

---

---

---

---

7



## Sustainability Compliance: Other Enforceable

### Traditional

- Purchase and sale agreements (transactions)
- Landlord / tenant contracts
- Product conformity

### More Recent

- More detailed supply chain code of conduct
- Human trafficking; human rights
- Greenhouse gas (GHG) emissions reporting

7/25/2024

©2024 Douglas Wilson Consulting, LLC

8

---

---

---

---

---

---

---

---

---

---

8



## Sustainability Compliance: Other Enforceable: **Newer/Emerging**

### Newer/ Emerging

- Reporting and disclosures: public; up & down the value chain
- Analyst ratings/ rankings
  - Report/ disclose via public channels the analysts rely on
  - Achieve minimum grade

How do these get created, implemented, monitored and reported?  
What are consequences of noncompliance?

7/25/2024

©2024 Douglas Wilson Consulting, LLC

9

---

---

---

---

---

---

---

---

---

---

9



### Sustainability Compliance: Standards, Frameworks

**Traditional**

- Carbon Disclosure Project (now CDP)
- Global Reporting Initiative (now GRI)
- OECD Due Diligence Guidelines
- UN Sustainable Development Goals

**More Recent**

- GHG Protocol
- Green Bond Principles
- SASB (Sustainability Accounting Standards Board - now ISSB)
- TCFD (Task Force on Climate-Related Financial Disclosures)
- EU Non-Financial Reporting Directive

©2024 Douglas Wilson Consulting, LLC

10

---

---

---

---

---

---

---

---

---

---



### Sustainability Compliance: Standards, Frameworks: **Newer/Emerging**

**Newer/ Emerging**

- Green Taxonomy; what qualifies as "green investment"
- EU Sustainability Reporting Standards (ESRS\*)
  - **Double materiality**
  - \* = Assurance required
- ISSB S1 and S2: **Global** (Brazil, Canada, Hong Kong, Japan, Mexico, Turkey, UK); ~half of non-US global economy
- TNFD (Task Force on **Nature** Related Financial Disclosures)

ISSB = International Sustainability Standards Board.  
 ISSB is an arm of the IFRS Foundation.  
 Several standards bodies merged into ISSB in late 2022, including SASB and CDP.

©2024 Douglas Wilson Consulting, LLC

11

---

---

---

---

---

---

---

---

---

---



### Sustainability Compliance: Voluntary Obligations

**Traditional**

- ISO certifications (9001, 14001)
- Energy Star
- Code of Conduct, general company commitments



**More Recent**

- B Corp; other credentials and certificates
- Best Places (to work, gender equity, most energy efficient, etc.)
- Sector/ Industry standards, frameworks
- Paris Climate Accords (2016)
- Goals and targets



7/25/2024

©2024 Douglas Wilson Consulting, LLC

12

12

---

---

---

---

---

---

---

---

---

---

## Compliance via Industry and Topical Standards and Frameworks



Each one establishes parameters and criteria for policy, procedures, and reporting. These obligations become compliance criteria.

7/25/2024

(c) 2024 Douglas-Hileman Consulting LLC

13

13

---

---

---

---

---

---

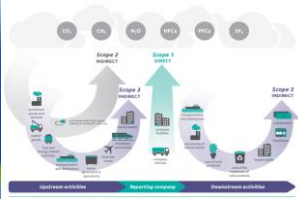
---

---

---

---

## GHG Protocol



Scope 1 = Direct emissions, from combustion  
 Scope 2 = Indirect emissions from purchase of energy  
 Scope 3 = All other indirect

Scope 3: Value Chain  
 Upstream: 8 categories  
 Downstream: 7 categories

GHG Protocol Corporate Standard  
 GHG Protocol Scope 2 Guidance  
 GHG Protocol Scope 3 Guidance  
 These and more at [www.ghgprotocol.org](http://www.ghgprotocol.org)

7/25/2024

©2024 Douglas-Hileman Consulting, LLC

14

14

---

---

---

---

---

---

---

---

---

---

## Sustainability Reporting Different Channels → Different Data Needs

### Data Needs : Examples

- How much water do we use? Where does it come from? Do our operations (or supply chain) impact scarce water resources?
- How much waste from our operations is recycled?
- How much of our raw materials has been recycled?
- What is the GHG emissions (in CO2e) inventory of the company?
- How much CO2e in the products you sell to Customer X?
- How much CO2e at the location in [country, state, or location]?
- What % of suppliers have code of ethics that meet or exceed our requirements? By number? By spend?
- Do suppliers pay fair wages?
- What is our progress towards goals?
- How can we improve ratings with analysts?
- How many customer requests do we get? Do we respond in time?
- What are safeguards to preserve IP?
- How do we know data is accurate and supportable?
- Is data reported via different channels the same? If not, why not?

7/25/2024

©2024 Douglas-Hileman Consulting, LLC

15

15

---

---

---

---

---

---

---

---

---

---





### Component 1: Control Environment



Principles	Perspectives and Common Gaps Involving IT
<ol style="list-style-type: none"> <li>1. Commitment to integrity and ethical values</li> <li>2. Independent Board of Directors oversight</li> <li>3. Structure, reporting lines, authorities, responsibilities.</li> <li>4. Attract, develop and retain competent people.</li> <li>5. People held accountable for internal control.</li> </ol>	<ul style="list-style-type: none"> <li>• Everyone is looking to the Board &amp; Exec. Mgmt.: reporting frameworks; investors; assurance providers; functional leaders.</li> <li>• The Board &amp; Exec. Mgmt. are looking at everyone else.</li> <li>• Cross-functional teams often used as component of governance.</li> <li>• Responsibility and accountability are assigned or assumed without making room for these new obligations. Parties may not have access or tools to fulfill responsibilities.</li> <li>• External parties may have key roles and need company data / info.</li> </ul>

---

---

---

---

---

---

---

---

---

---

22

### Component 2: Risk Assessment



Principles	Perspectives and Common Gaps Involving IT
<ol style="list-style-type: none"> <li>6. Clear objectives specified.</li> <li>7. Risks identified to achievement of objectives.</li> <li>8. Potential for fraud considered.</li> <li>9. Significant changes identified and assessed.</li> </ol>	<ul style="list-style-type: none"> <li>• Compliance drivers originate from new and different channels. Compliance obligations don't make it into ERP or internal systems.</li> <li>• Compliance and reporting requirements vary by stakeholder for the same topic.</li> <li>• Data / information can be subject to manipulation.</li> <li>• Externally-driven changes can be direct (regulatory) or indirect (customer, trade association).</li> <li>• Linkage between internal changes and Sustainability compliance/ reporting may not be recognized, or access to data may not be possible.</li> </ul>

---

---

---

---

---

---

---

---

---

---

23

### Component 3: Control Activities



Principles	Perspectives and Common Gaps involving IT
<ol style="list-style-type: none"> <li>10. Control activities selected and developed.</li> <li>11. General IT controls selected and developed.</li> <li>12. Controls deployed through policies and procedures.</li> </ol>	<ul style="list-style-type: none"> <li>• Companies may create procedures from scratch, b/c process owners are not aware (or do not have access) to others that could be building blocks.</li> <li>• Control activities can be required into the value chain - beyond what the organization "controls": Access controls.</li> <li>• GHG emissions may need to be recalculated for prior reporting periods; management of this process.</li> <li>• "Lockdown" of work papers supporting Sustainability reporting and disclosures.</li> <li>• Policies and procedures may be externally reported or disclosed, and subject to review/ audit/ assurance by other parties.</li> <li>• Content can include intellectual property.</li> <li>• IT: build or buy? Many offerings, most still evolving.</li> </ul>

---

---

---

---

---

---

---

---

---

---

24







### Roundtable Topic #3: Now What?



- Where can IT take a greater role in Sustainability compliance and/ or reporting?
- What aspect of today's content is of most interest to you?

REQUEST: Please provide comments via the Chat function.

7/25/2024

©2024 Douglas Hileman Consulting, LLC

28

28

---

---

---

---

---

---

---

---

---

---



#### Douglas Hileman, FSA, CRMA, CPEA, P.E.

Doug helps clients with compliance, risk, reporting, audits, and assurance readiness in the Sustainability space. He is an author of the COSO ICSR supplemental guidance document. His tailored workshops have been appreciated for Compliance, Internal Audit, company in-house teams, procurement functions.

He works directly with clients, and as a specialist supporting accounting firms and boutique consultancies. He draws on 40+ years of experience, including in industry, "second line auditing" (environmental, safety, sustainability), six years at a Big 4 firm, supporting Internal Audit and external assurance. He was the senior environmental management and environmental auditing specialist on the Volkswagen Monitor Team.

He presented and contributed to IIA, Compliance Week, SCCE, and other professional associations, firms, and companies.

For more, see [www.douglashileman.com](http://www.douglashileman.com)  
See also [www.auditreadinesspro.com](http://www.auditreadinesspro.com)

7/25/2024

©2024 Douglas Hileman Consulting, LLC

29

29

---

---

---

---

---

---

---

---

---

---