



# Auditing Fundamentals

Compliance

# Business Needs



Photo by Kindel Media from Pexels



Photo by Tom Fisk from Pexels



**Do we have to?**

# Regulations

- + PCI DSS
- + HIPAA
- + GDPR
- + CPPA
- + SOX

# PCI DSS

---

## Payment Card Industry Data Security Standard

- + Mandated by card brands
- + Administered by the Payment Card Industry Security Standards Council
- + Created to increase controls around cardholder data to reduce credit card fraud



# HIPAA

---

## Health Insurance Portability and Accountability Act of 1996

- + US regulations for the use and disclosure of Protected Health Information (PHI)
- + The Final Rule on Security Standards was issued on February 20, 2003
- + Standards and Specifications
  - + Administrative Safeguards
  - + Physical Safeguards
  - + Technical Safeguards



# GDPR

---

## General Data Protection Regulation

- + Data protection and privacy law in the European Union (EU) and the European Economic Area (EEA)
- + Controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles



# CPPA

---

## California Consumer Privacy Act

- + Intended to enhance privacy rights and consumer protection for residents of California, United States.
- + Companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages.
- + Liability may also apply in respect of businesses in overseas countries who ship items into California.





# SOX

---

## Sarbanes–Oxley Act of 2002

- + US federal law mandates certain practices in financial record keeping and reporting for corporations.
- + Requires strong **internal control processes** over the **IT infrastructure** and **applications** that house the **financial information** that **flows into its financial reports** in order to enable them to make **timely disclosures** to the public **if a breach were to occur**.





**How do we do it?**