What is a BISO?

Essentially, it is the person responsible for defining and (or) messaging the security program for a business area (or department).

It's a Person

Security Ambassador

Security Champion

It's also a Program

Business Information Risk

Central or Decentral

Central – may be responsible for multiple areas and extends security principles

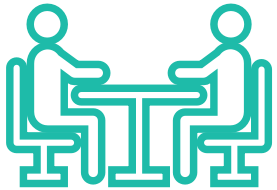
Decentral – may be responsible for technology and other control functions

yass partners

It’s the “branding” and “perception” of security

The BISO helps us better understand…

Employee risk



What happens in each business area (and what to protect and how it's used)

Security Program Compliance

Business Information Risk

1. Communication & Adoption
2. Risk Assessment & Measurement

Business Information Risk

Communication & Adoption

1

Messages FROM Security

Security Policies & Standards

Compliance updates

-Vulnerability Management

-Incident Escalations

Training

-General Security Best Practices

-New Controls and Process changes

2

Front door TO Security

Common Requests

-Client RFP

-Audit / Regulatory Review

-Security Assessment Training

-Ad hoc Inquiry

3

Business Advocate

How does the department consider security

What are the critical and sensitive information assets (aka: Crown Jewels)

yass partners

Business Information Risk

Risk Assessment & Measurement

1

Risk Reviews

Risk Assessments for department specific requests

-Third party / vendor risk

-New functionality

This could be embedded in engineering / development functions as it relates to design, review, promote

2

Mitigation Plans

Documents and tracks risk mitigation and action plans

Creating and proposing mitigation strategies

3

KPI / KRI Tracking

Report and track security metrics aligned to the business

Regular review of performance thresholds (RAG)