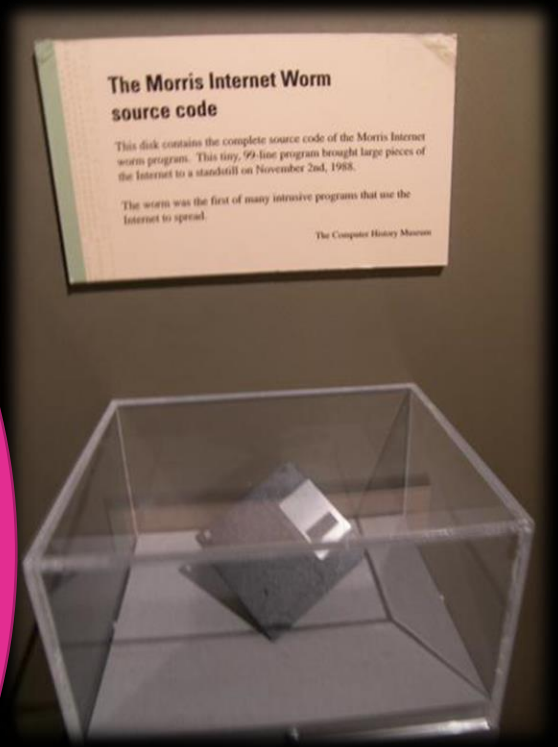
Alyssa

MILLER

The “B” is for Business

Driving Practical Security Through the BISO

Some useless Infosec trivia



?

Hacker and Researcher

16 years in security roles

Author and Podcaster

BISO - S&P Global Ratings

https://alyssasec.com

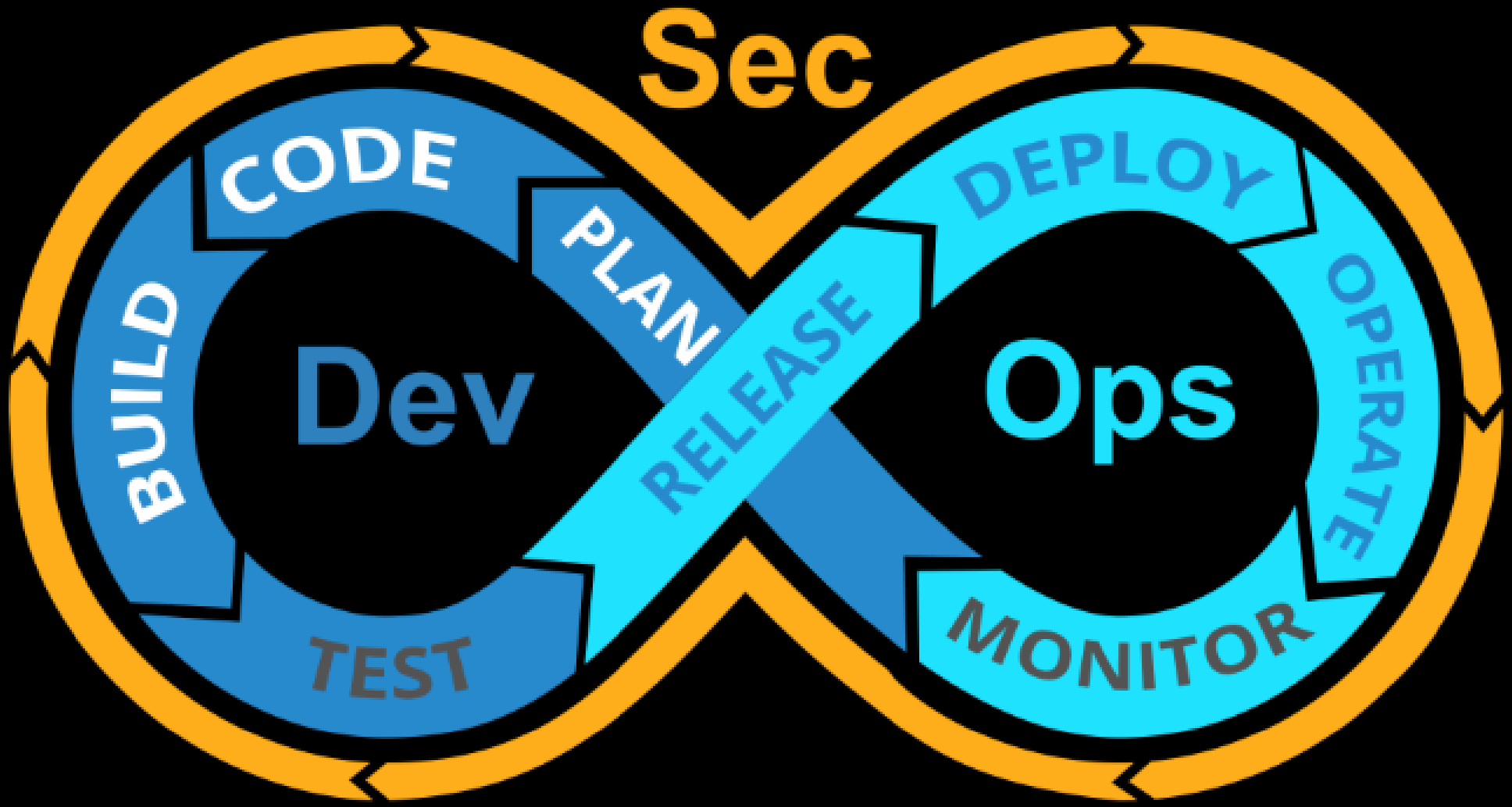
BISO

Business Information Security Officer

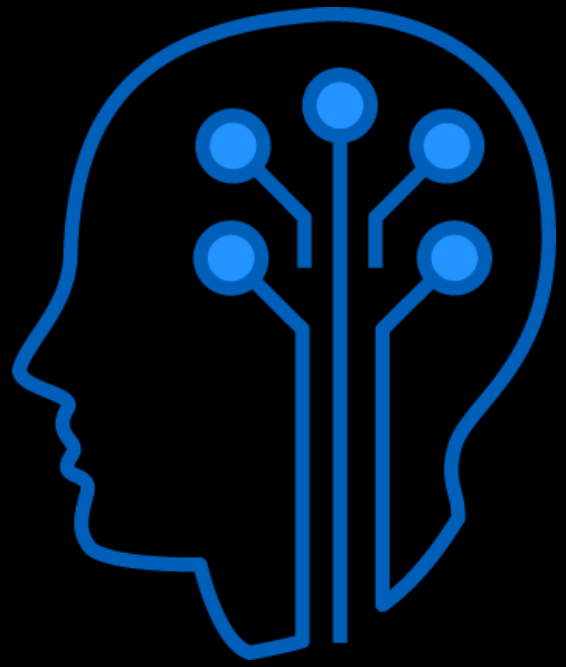
Information Security

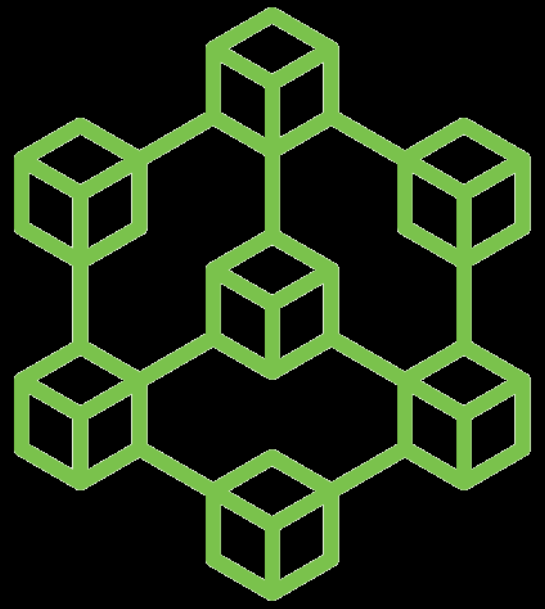
The Business Lines

Advocating for security within the business line

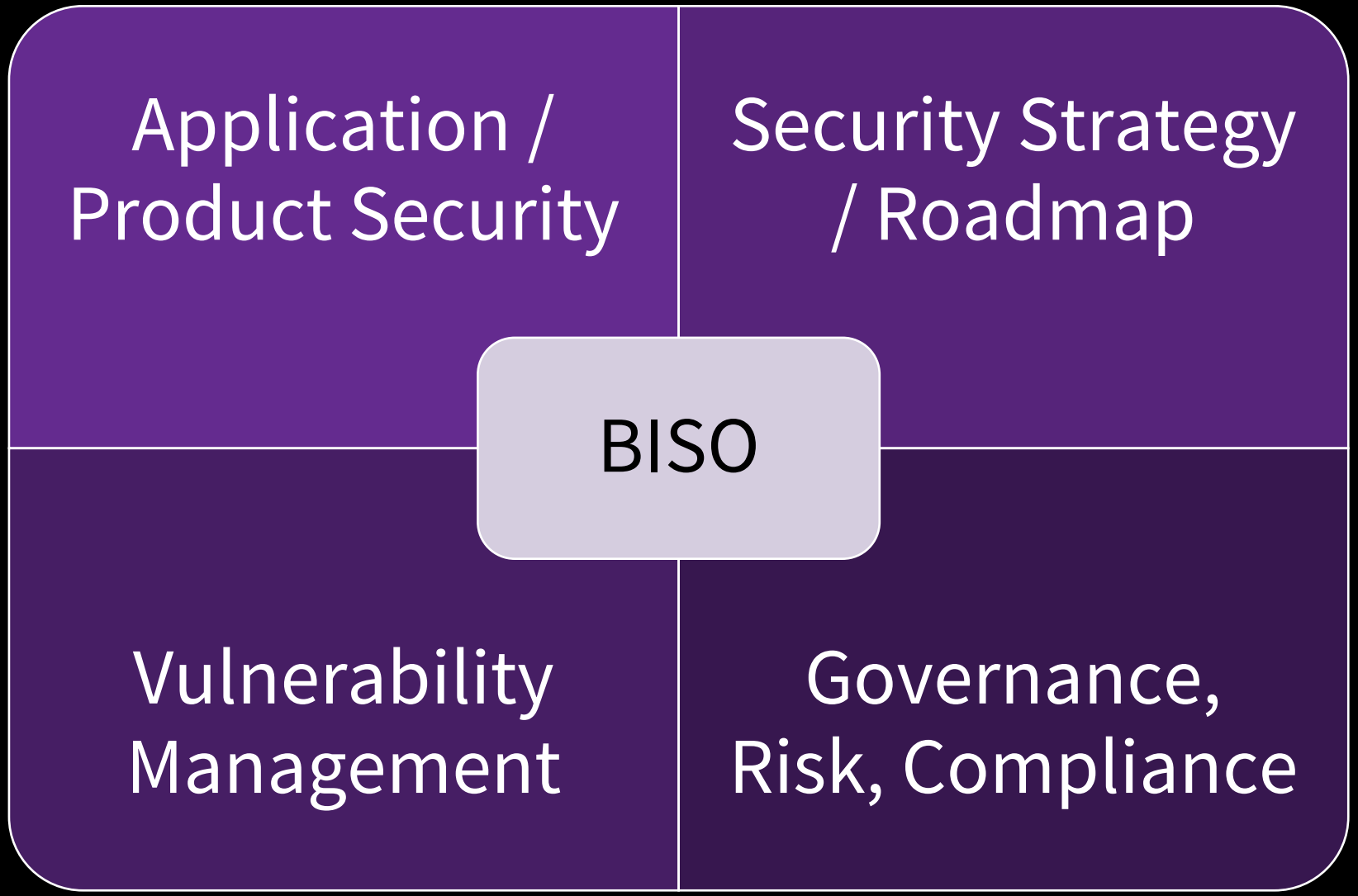


Advocating for the business with the security team





The BISO's Responsibilities

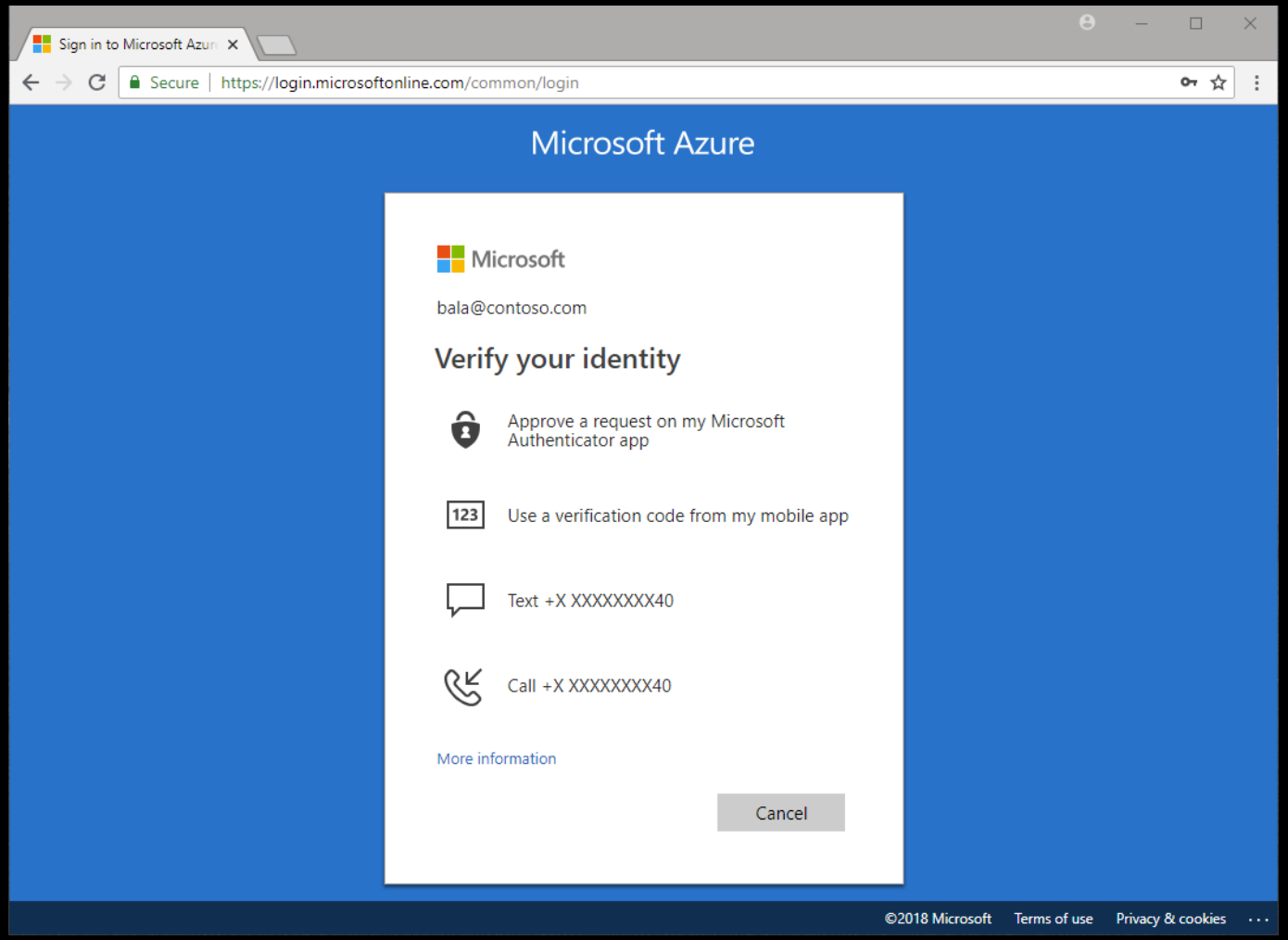


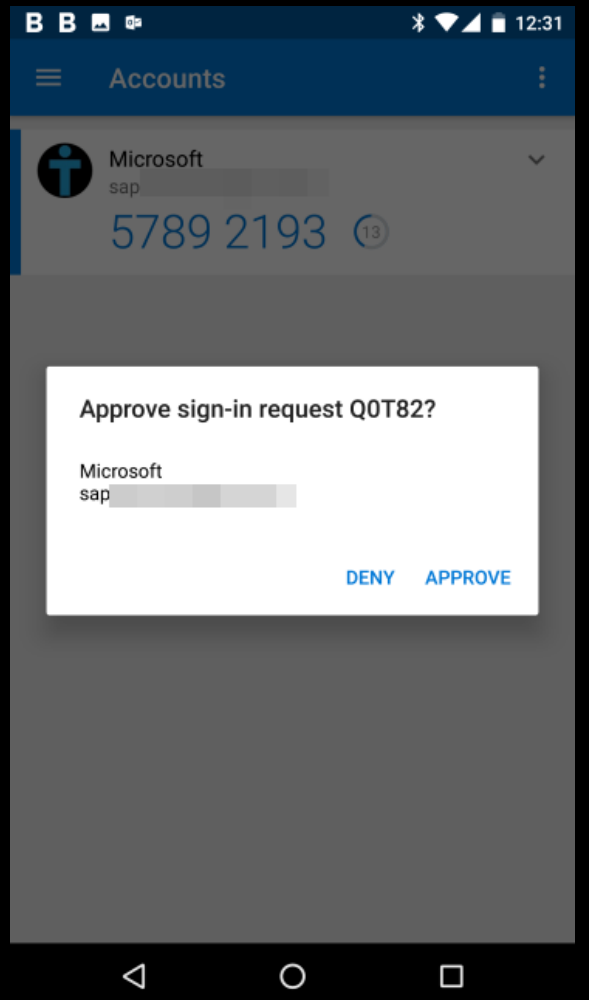
Qualities of a Good BISO

Winning With the BISO

Benefits of the BISO function: Winning Funding

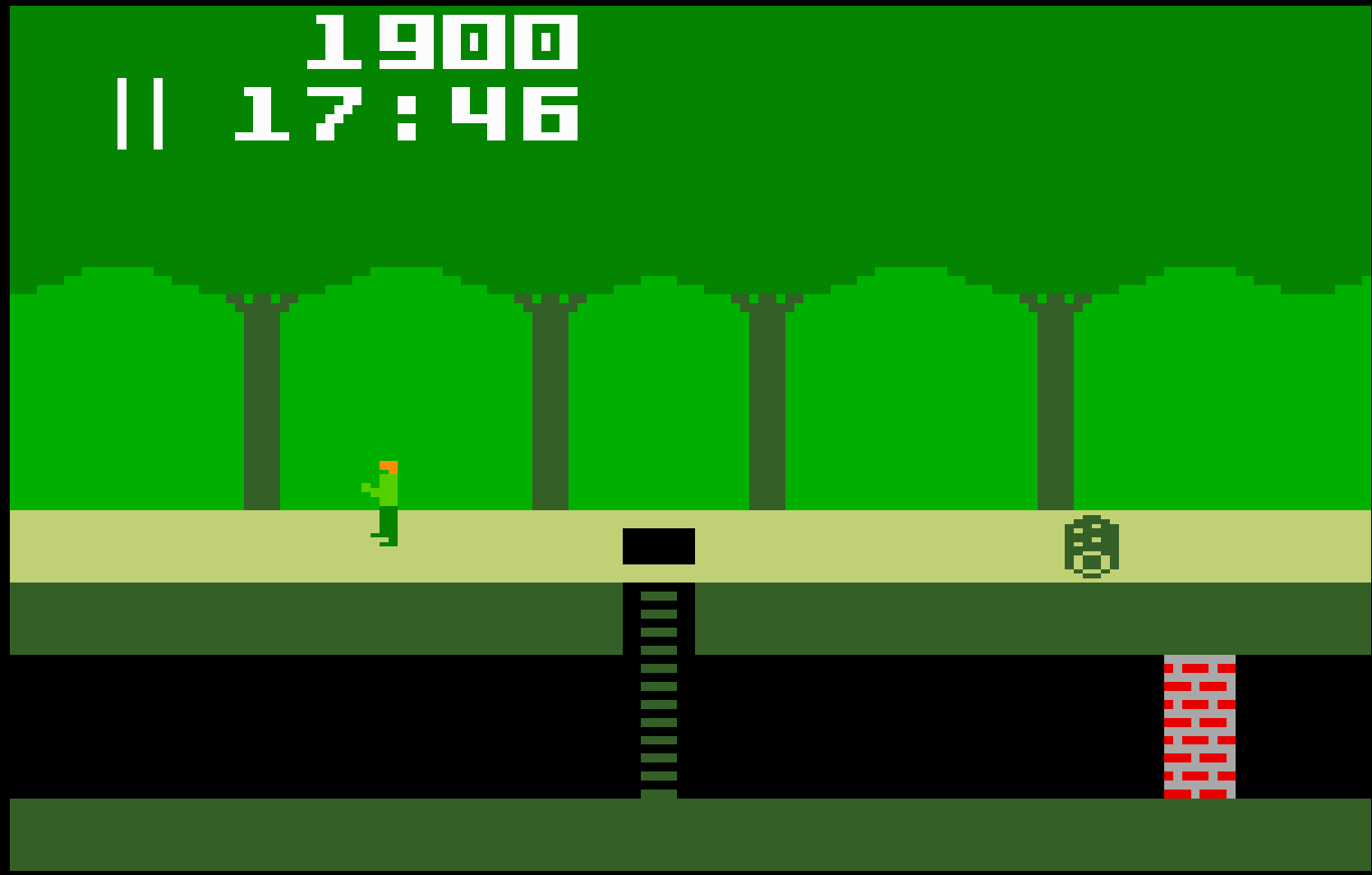
Benefits of the BISO function: Improved Adoption



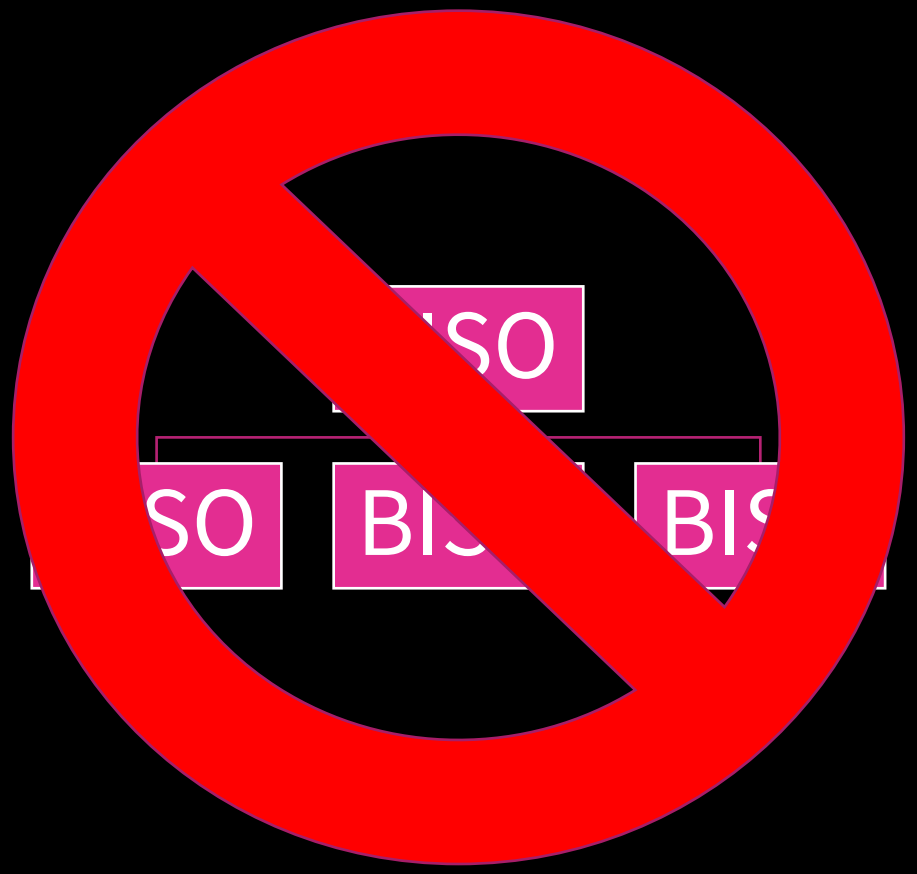


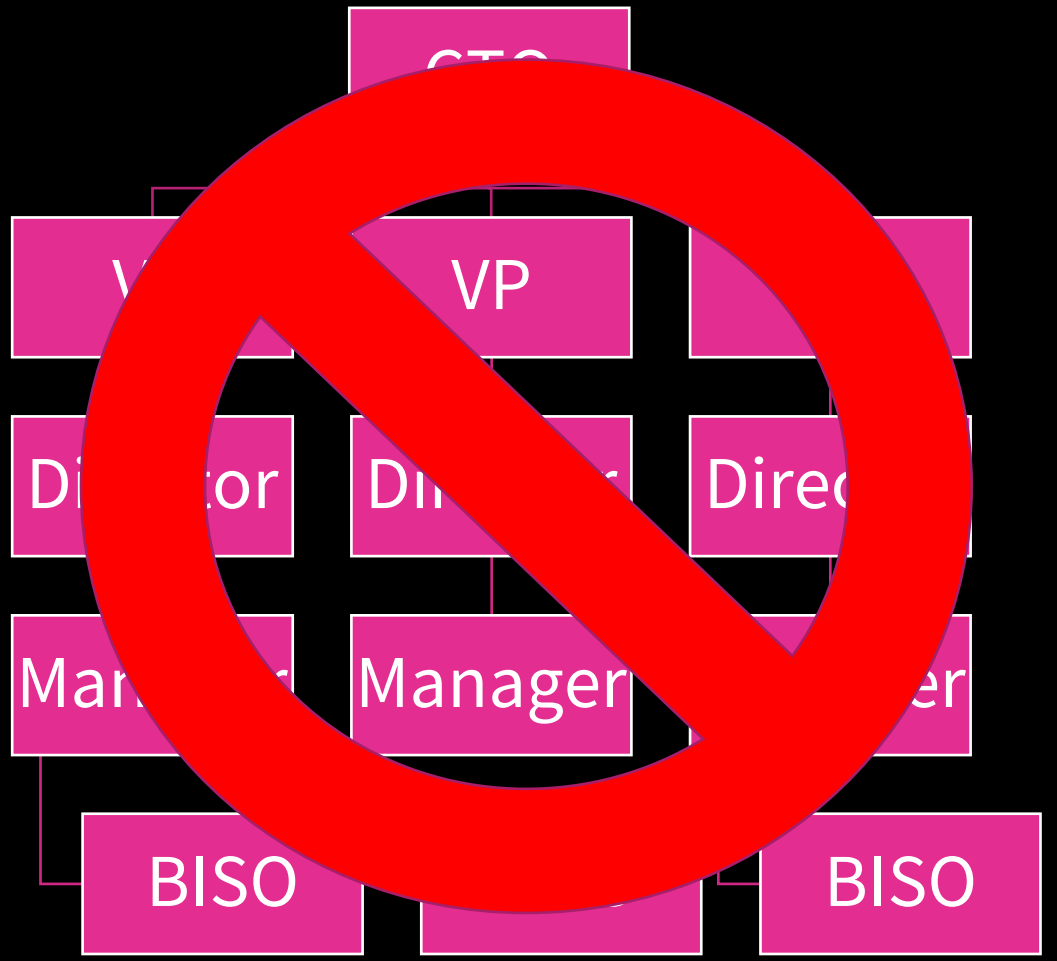
Benefits of the BISO function: Program Effectiveness

Potential Pitfalls

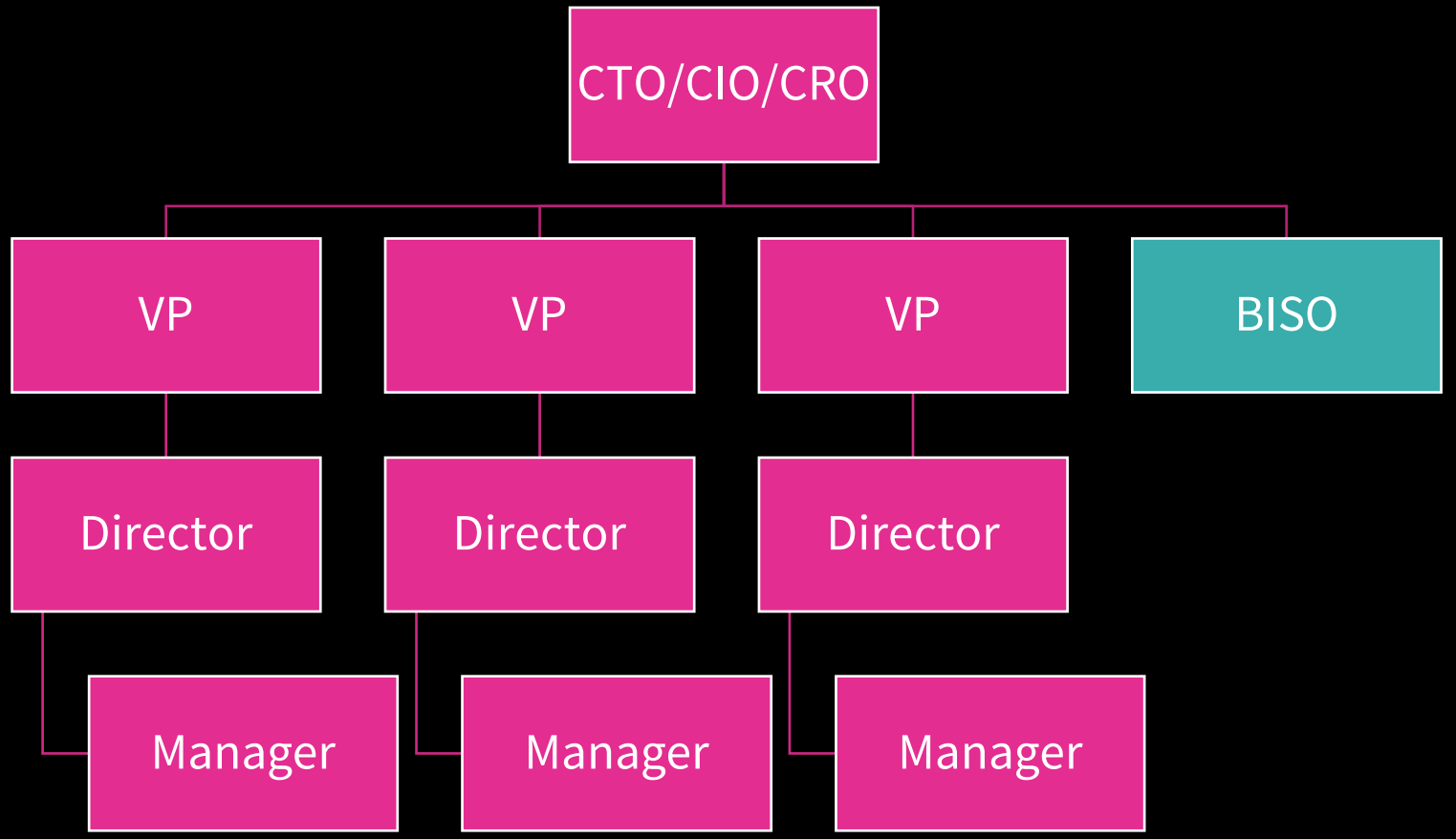


Common Mistakes: Reporting Structure

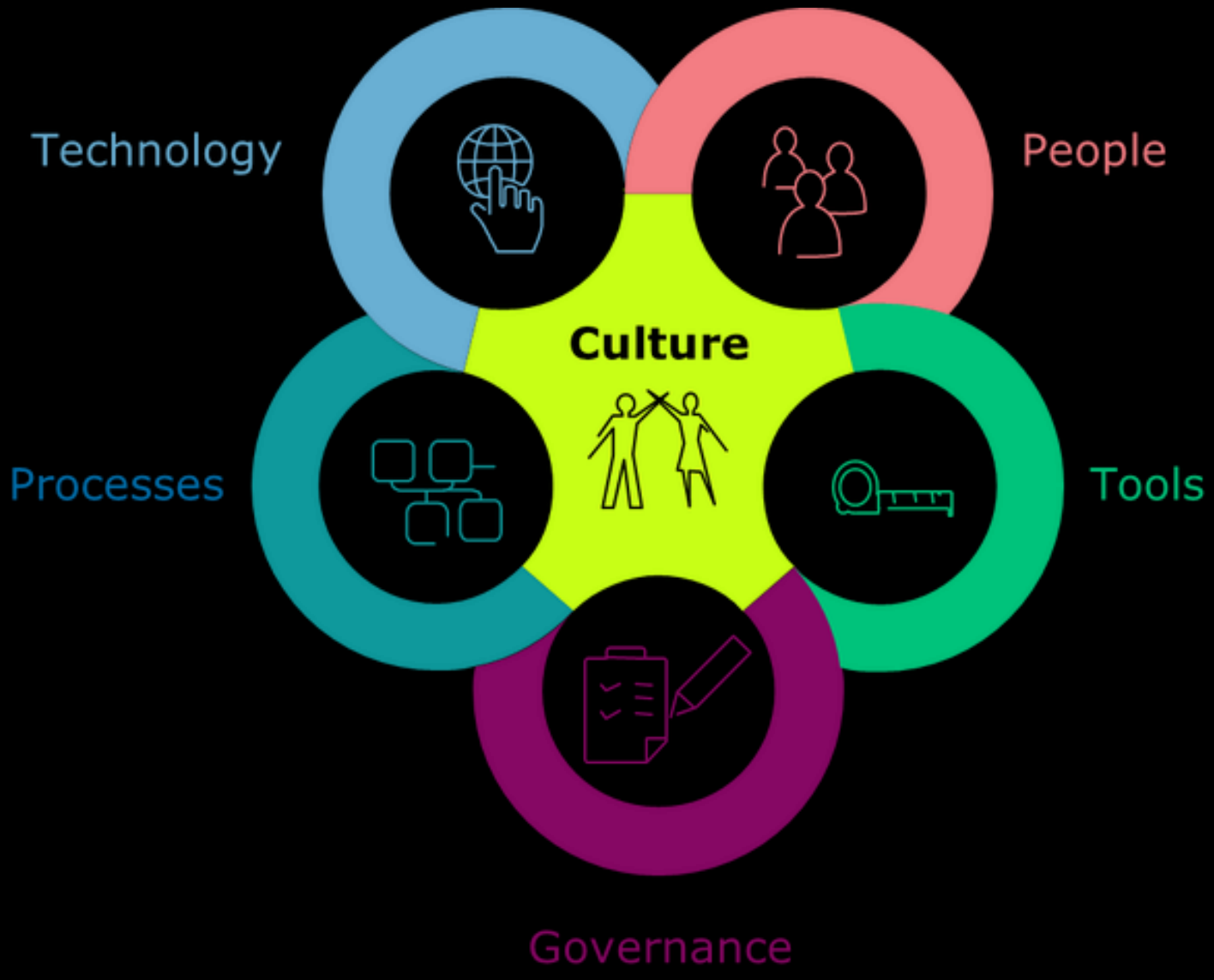




Common Mistakes: Reporting Structure



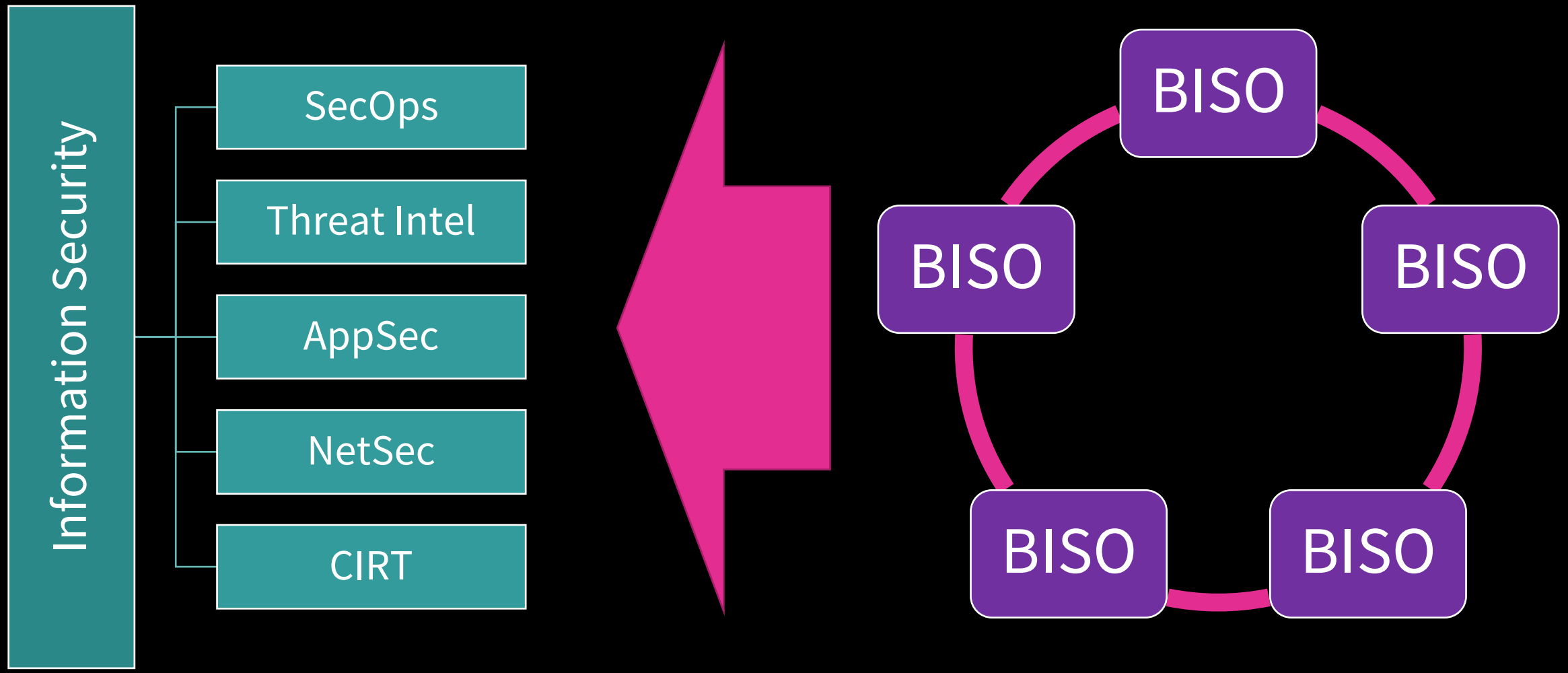
Common Mistakes: Tactical Focus



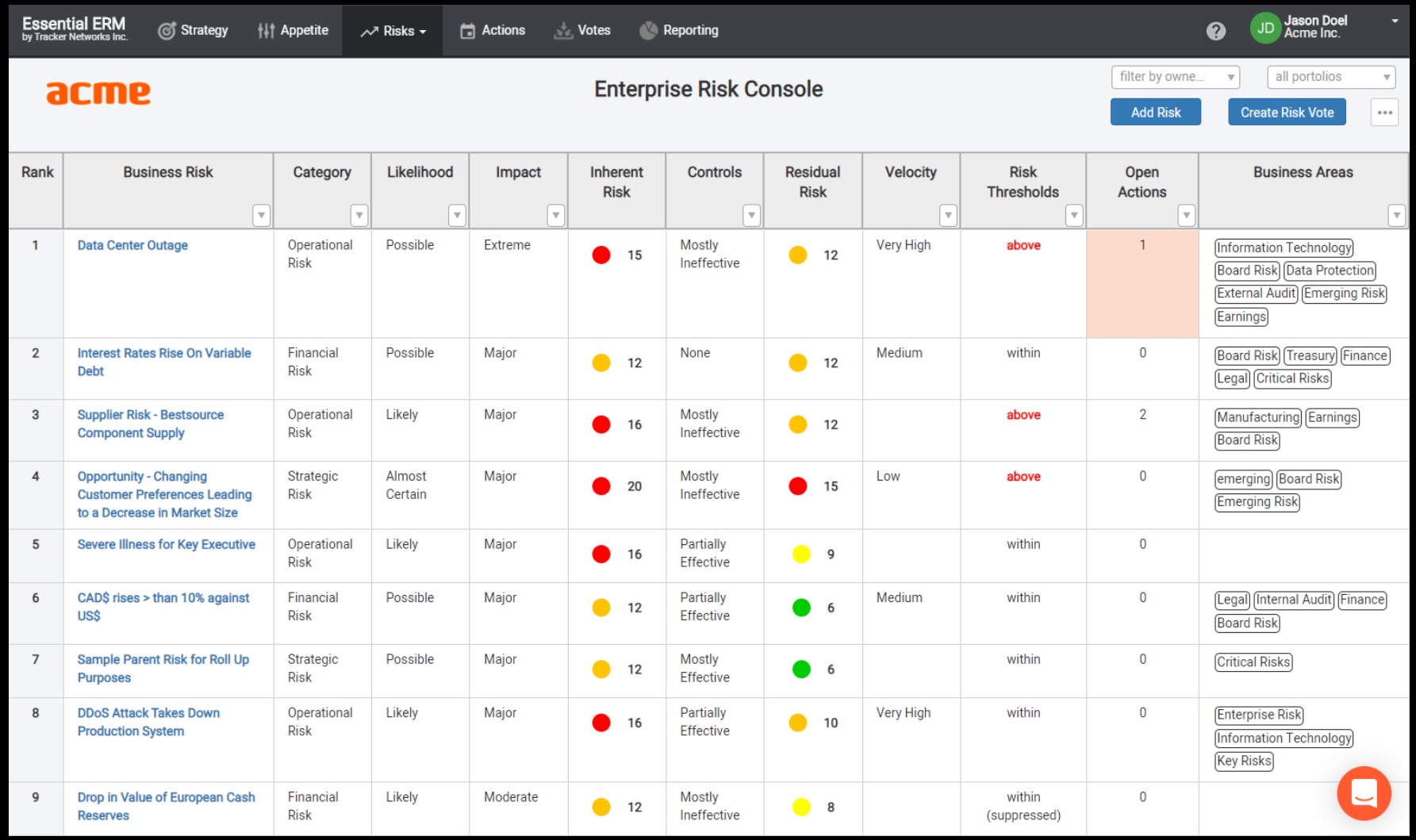
Common Mistakes: Lack of Visibility

Best Practices

Best Practices: Build a BISO Community



Best Practices: Identify and Update Top Risks



Rank	Business Risk	Category	Likelihood	Impact	Inherent Risk	Controls	Residual Risk	Velocity	Risk Thresholds	Open Actions	Business Areas
1	Data Center Outage	Operational Risk	Possible	Extreme	15	Mostly Ineffective	12	Very High	above	1	Information Technology, Board Risk, Data Protection, External Audit, Emerging Risk, Earnings
2	Interest Rates Rise On Variable Debt	Financial Risk	Possible	Major	12	None	12	Medium	within	0	Board Risk, Treasury, Finance, Legal, Critical Risks
3	Supplier Risk - Bestsource Component Supply	Operational Risk	Likely	Major	16	Mostly Ineffective	12		above	2	Manufacturing, Earnings, Board Risk
4	Opportunity - Changing Customer Preferences Leading to a Decrease in Market Size	Strategic Risk	Almost Certain	Major	20	Mostly Ineffective	15	Low	above	0	emerging, Board Risk, Emerging Risk
5	Severe Illness for Key Executive	Operational Risk	Likely	Major	16	Partially Effective	9		within	0	
6	CAD$ rises > than 10% against US$	Financial Risk	Possible	Major	12	Partially Effective	6	Medium	within	0	Legal, Internal Audit, Finance, Board Risk
7	Sample Parent Risk for Roll Up Purposes	Strategic Risk	Possible	Major	12	Mostly Effective	6		within	0	Critical Risks
8	DDoS Attack Takes Down Production System	Operational Risk	Likely	Major	16	Partially Effective	10	Very High	within	0	Enterprise Risk, Information Technology, Key Risks
9	Drop in Value of European Cash Reserves	Financial Risk	Likely	Moderate	12	Mostly Ineffective	8		within (suppressed)	0	

Best Practices: Vision, Mission, Values, and Roadmap

VISION

Foster a culture in which cyber security strategy aligns with business objectives to enable innovation

MISSION

Bring cyber security context to strategic planning and operations. Enhance capacity and efficiency by building a bridge to Information Security and help shape corporate security strategy to align with the business

VALUES

- Cybersecurity's value is derived from business enablement
- Frictionless enablement is core to success
- Security conscious culture requires focus on people, process, technology, and governance
- Uniting development, security, and operations under common goals is foundational

Best Practices: Regular Executive and Board Updates

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa
MILLER

@alyssam_infosec

https://alyssasec.com