FENWICK
& WEST

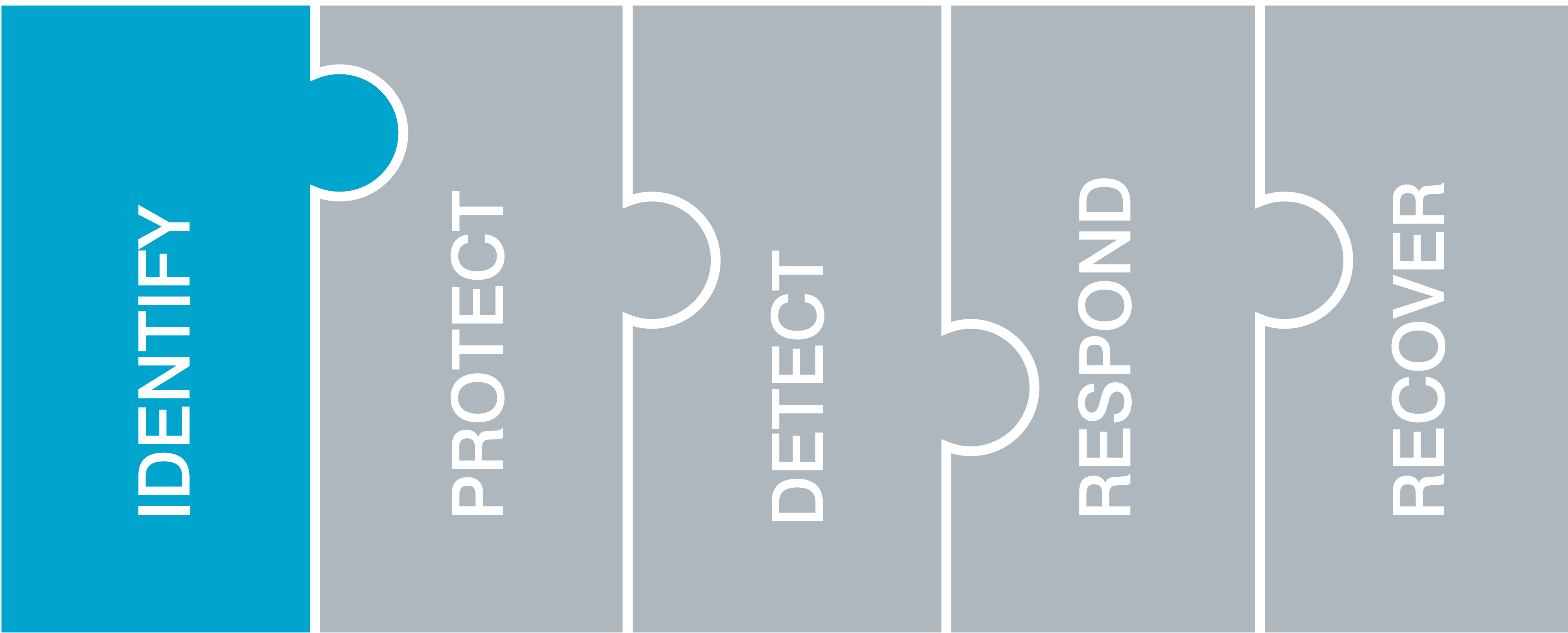
Top 10 Best Practices for Handling a Data Breach

IDENTIFY

1 Conduct a Readiness Assessment using an industry standard framework such as the NIST Cyber Framework

2 Develop a cybersecurity and information governance charter

3 Inventory, classify, and risk-rank critical systems and assets

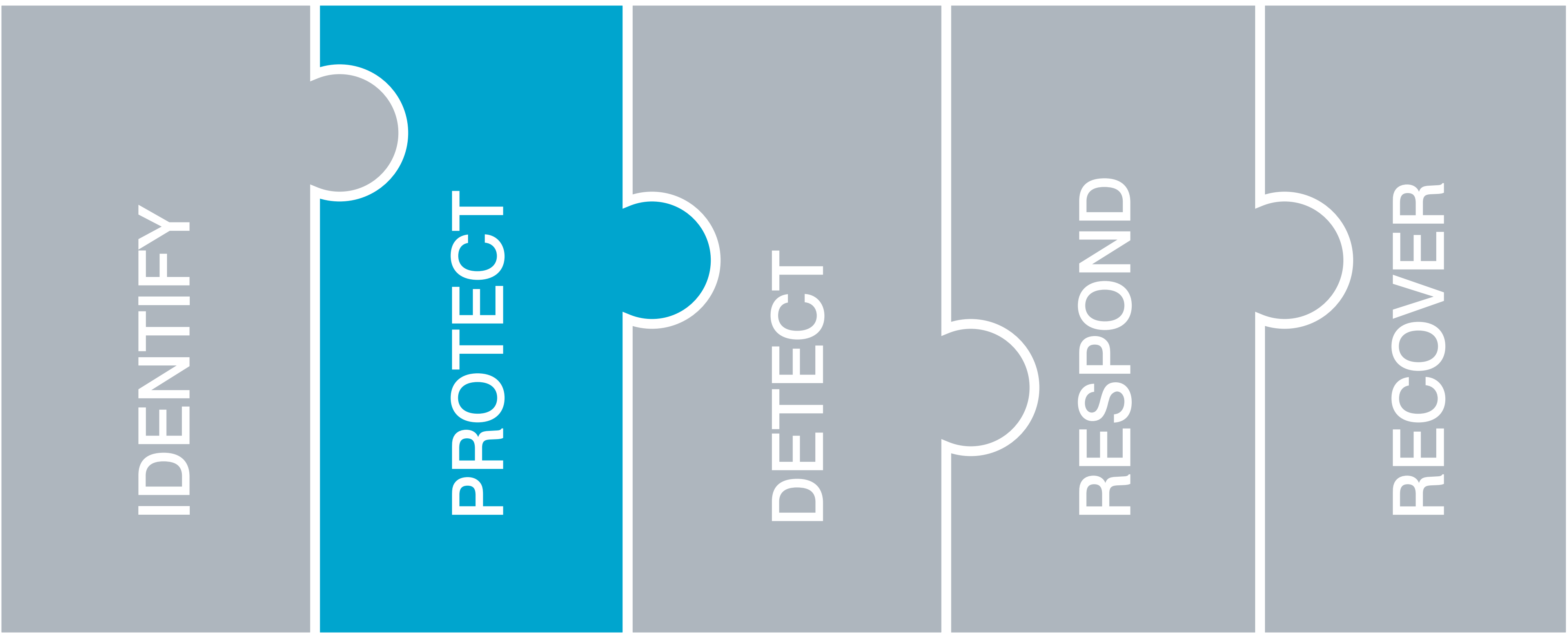


PROTECT

4 Subscribe to anticipatory threat intelligence services; Participate in cyber information sharing

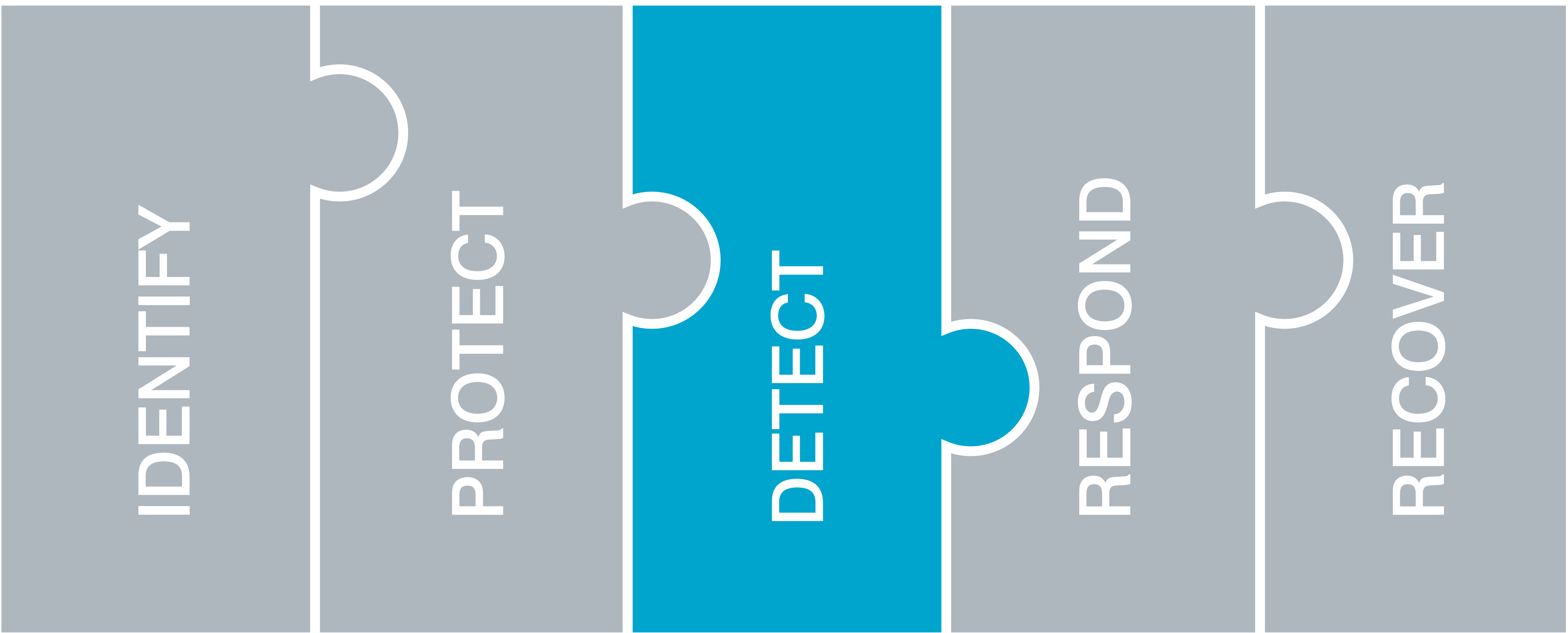
5 Provide general and role-based training

6 Build vendor assessment process and enhance contractual protections



DETECT

7 Scan for advanced persistent threats and malware



IDENTIFY

PROTECT

DETECT

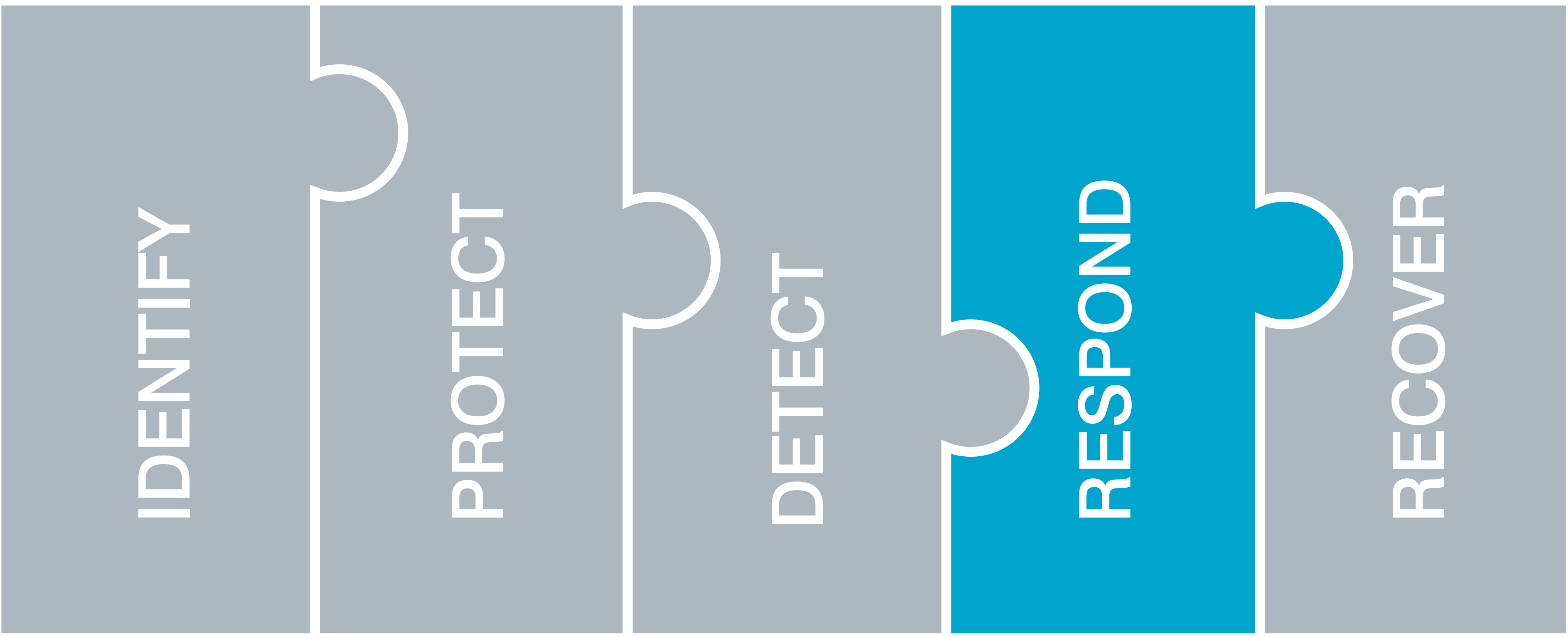
RESPOND

RECOVER

RESPOND

8 Develop and periodically update incident response plans

9 Test incident response with a war game



IDENTIFY

PROTECT

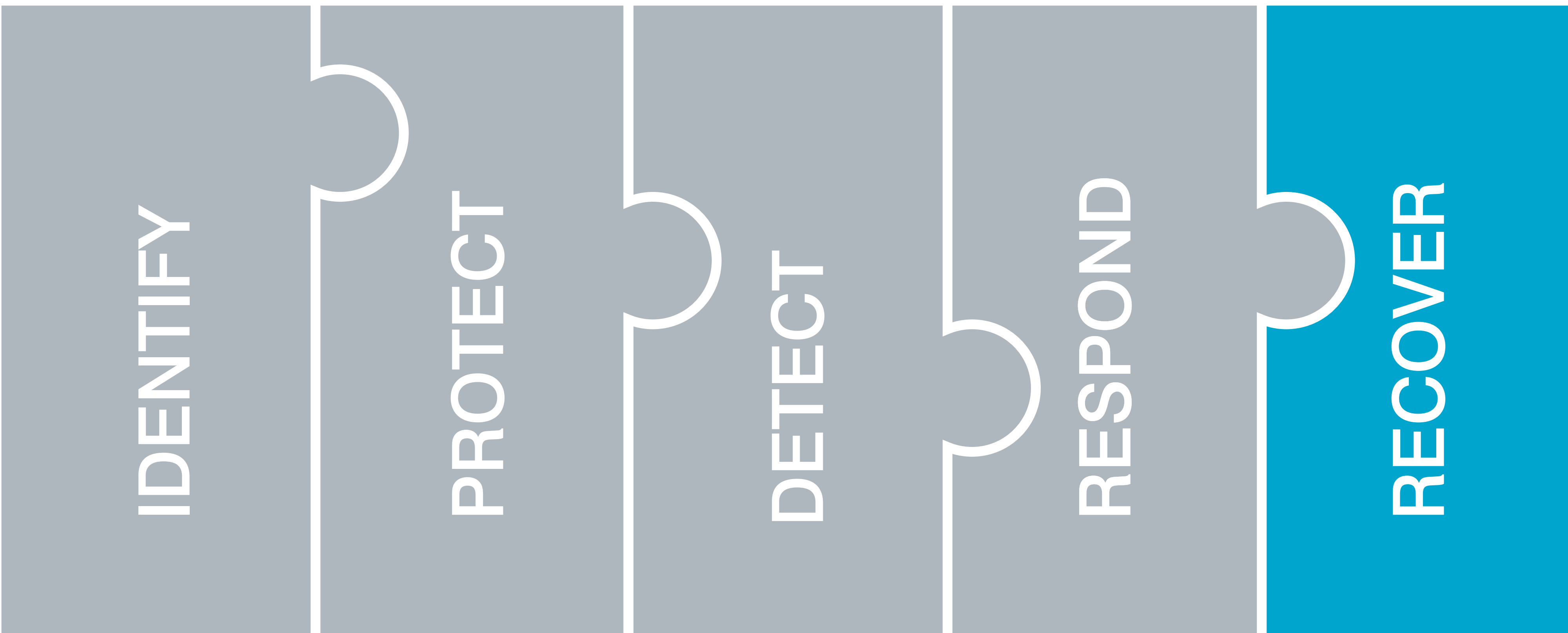
DETECT

RESPOND

RECOVER

RECOVER

10 Update security baselines and data protection policy suite as needed



KEY POLICIES AND BEST PRACTICES

Incident response plan – define roles and determine available resources

Security awareness training and testing (vulnerability scanning and penetration testing)

Diligence and contractual protections from third-party vendors

Industry standard practices (access control, encryption, multi-factor authentication, patching)

SEC filings: disclose risk factors tailored to your business

Click to read our latest Privacy Bulletin