

简称	英文	中文	备注	页数
BC	Business Continuity	业务连续计划		70、74
DR	Disaster Recovery	灾难恢复计划		70、74
RTO	Recovery Time Object	恢复时间目标	RTO是指灾难发生后，从IT系统宕机导致业务停顿之刻开始，到IT系统恢复至可以支持各部门运作，业务恢复运营之时，此两点之	71、77
RPO	Recovery Point Object	恢复点目标	是指灾难发生后，容灾系统能把数据恢复到灾难发生前时间点的数据。	71、77
IR	Incident Response	事件响应	件响应计划来管理组织将如何调查安全攻击	106
SSDLC		软件开发生命周期		115
SAST		静态应用程序安全测试		117、118、123、151
DAST		动态应用程序安全测试		117、118、123、151
DLP		数据丢失防护	数据丢失防护(DLP)是通过监视本地系统、网络、电子邮件和其他流量来监控和保护员工访问的数据的方法。	125、126、133
DRM		数据版权管理		133
ERM		企业风险管理		133

IAM		身份、权利以及访问管理		135
IdM		身份管理		137
MFA		多因素认证		73、138、144 、145、146
FIDO	Fast Identity Online	线上快速身份验证联盟		144
RBAC	Role-Based Access Control	基于角色的访问控制		145
ABAC		基于属性的权限控制	是通过动态计算一个或一组属性来是否满足某种条件来进行授权判断	145
SecaaS		安全即服务	提供商提供安全能力作为云服务	147
PII	personally identifiable information	个人身份信息保护	有关一个人的任何数据，这些数据能帮助识别这个人，如姓名、指纹或其他生物特征资料、电子邮件地址、电话号码或社会安全	152