CERTIFIED CISO BODY OF KNOWLEDGE FRAMEWORK **BUSINESS ENABLEMENT** Domian 3 Domain 4 Domain 1 & 3 Domian 5 Domian 4 Domian 1, 2 & 5 **PROJECT DELIVERY** LIFECYCLE **MOBILE COMPLIANCE MERGERS AND CLOUD PROCESSES TECHNOLOGIES** COMPUTING **AND AUDITS ACQUISITIONS** Requirements Internal/external audit BYOD HR/On Boarding/ Termination Design management Endpoint detection and Acquisition Risk Cloud Architecture Regulatory compliance **Security Testing Business Partnerships** response Assessment Strategy and Guidelines International standards Sensitive data Business Continuity and Disaster Recovery Maintenance alignment Integration Cost management **Cloud Risk Evaluation** Vendor/customer audit User behavior monitoring **Security Awareness** management Domian 3 & 4 Domian 1, 4 & 5 Domian 3 **SECURITY SAAS POLICY BUSINESS ARCHITECTURE ENABLEMENT PROGRAM AND GUIDELINES SECURITY MANAGEMENT** SON SON COMPLIANCE Technical orchestration **ARCHITECTUF AND AUDITS** Vendor assurance Minimize failure surface Governance Security functionality Engineering and Personnel/automation balance Testing and integration implementation Compliance and audit Monitoring and alerting Lifecycle management **RISK** Risk identification **DELIVERY MANAGEMENT LIFECYCLE** Security operations Domian 1 & 5 Risk program governance Asset inventory view Domian 5 **RISK MANAGEMENT EC-Council** Clear risk metrics Risk results **PROGRAM IDENTITY** management Risk communications **Building A Culture Of Security MANAGEMENT MANAGEMENT BUDGET** Assessment Business risk advisement management **CISO Role** Assessment coordination ROI analysis Third-Party Risk Management & Risk Quantification Overview Risk prioritization → Talent retention **BUDGET INCIDENT** Balanced management MANAGEMENT **Cost Reduction THREAT STRATEGIC** PREVENTION 8 **PLANNING DETECTION** LEGAL AND HUMAN Domian 4 RESOURCES Domian 4 Domian 4 **IDENTITY MANAGEMENT** Domian 5 **THREAT PREVENTION &** Domian 1, 4 & 5 **INCIDENT DETECTION MANAGEMENT T** Account Creation / STRATEGIC **LEGAL AND** Log Analysis/Correlation/SIEM Deletions **PLANNING HUMAN RESOURCES** Alerting (IDS/IPS,FIM,WAF Incident Response Single Sign On (SSO, Antivirus, etc) Simplified Sign on) Tactical, intermediate, Media Relations Netflow Analysis Data Discovery and strategic planning Repository (LDAP/Active Network/Application Incident Readiness Directory) Vendor Contracts Strategy communication Firewalls Federated IAM Forensic Investigation Investigation /Forensics Alignment to the business Vulnerability ManagementApplication Security Privilege Access Threat Intelligence Management