Security Checklist

As the cyber security adapts and evolves, organisations need to implement a program of risk-based controls and practices to reduce exposure, manage present, identify perceived and predict potential impacts from cyber breach or attack.

Creating a base level of security through a strong foundation of cyber principles, policies, procedures and people, can ensure performance, productivity and protection for your organisation and enable you to achieve compliance and insurance objectives.

We've created this infographic to guide you through the minefield of information around cyber compliance and insurance. These are the key areas for you to consider:

Education & Awareness

Assurance

Identity and Access Management

Communications & Network Security

Application and Asset Protection

Secure Cloud

Compliance and Documentation

Change Management

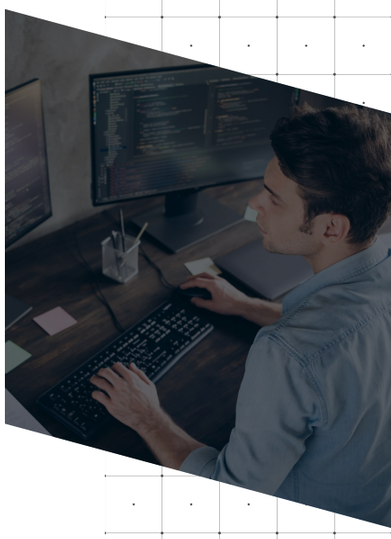
Education & Awareness

Tackling the front-line is where your education programs will achieve the greatest impact – everyone needs to know more than they do today. Cyber training and awareness can help protect your business from unnecessary exposure to risk.

- ☐ Educate throughout an employee lifecycle (not just at the beginning).
- ☐ Schedule regular updates, automate reminders and link KPI's to track completion
- ☐ Craft tailored programs for employee role types and grades
- ☐ Identify and share goals, risks and security policies with the team
- ☐ Update training content regularly to stay relevant and compliant

Assurance

Independent testing and incident simulations ensure networks and applications are secured. Understanding the effectiveness of existing measures enables pro-active management and monitoring of vulnerabilities - and improves responsiveness.



- ☐ Create and maintain a Cyber Security Incident response plan
- ☐ Obtain Cyber Incident Insurance
- ☐ Organise and execute incident simulations to test security maturity
- ☐ Regularly review and harden security technology policies and controls
- ☐ Validate controls with regular penetration testing
- ☐ Gather intelligence to understand and interpret the threat landscape
- ☐ Schedule regular updates to ensure currency and compliance
- ☐ Ensure logs and alerts are reviewed and events responded to, using SIEM and SOC capabilities
- ☐ Create and share a Disaster Recovery (DR) plan
- ☐ Engage stakeholders and operational teams in rollout of DR and Business Continuity Plan (BCP)
- ☐ Test and review processes and iterate as needed

Identity and Access Management

Understanding, documenting, and managing user accounts, privileges and access levels will help you identify weak links and risks across your organisation.

- [ ] Document user accounts and privileges
- [ ] Manage privileged access carefully
- [ ] Implement Multi-Factor Authentication (MFA)
- [ ] Evaluate and re-align responsibilities and access levels
- [ ] Create supporting processes and procedures for Identity and Access Management
- [ ] Use single sign-on (SSO) to authenticate users for multiple platforms
- [ ] Deploy VPN's or Zero Trust for remote access to information resources

Communications & Network Security

Preventing attack and retaining productivity in the face of cyber breach demands a thorough review of security protocols and risks from the outside, and inside of your organisation.

- [ ] Deploy a comprehensive security architecture including:
  - [ ] Email security
  - [ ] Endpoint security
  - [ ] Perimeter and network security
  - [ ] Cloud security
  - [ ] Data security
- [ ] Undertake a full internal and external review of potential threats and opportunities
- [ ] Build and deploy a best practice approach to data management and protection
- [ ] Configure systems and technologies to protect operations and retain productivity
- [ ] Prevent or limit network and information access from unknown and unmanaged devices
- [ ] Set up a security perimeter on your cloud architecture
- [ ] Review, approve and review access levels and delegations of authority regularly

Application and Asset Protection

Maintaining a real-time directory of assets and security risks is the first step in truly understanding the landscape and profile of cyber risk across your organisation – and the driving force behind your future security strategy.

- [ ] Use technology and talent to document your network and your assets.
- [ ] Evaluate the current technologies and teams tracking IT assets
- [ ] Implement a Vulnerability Management program to independently identify and track risk
- [ ] Utilise identified risks as opportunities to improve security posture
- [ ] Evaluate your backup and recovery policy
- [ ] Implement asset /application usage and access parameters at all levels
- [ ] Review and update patching, passwords and people policies
- [ ] Ensure remediation activities and responsibilities are clearly defined
- [ ] Evaluate and educate team members of updates and accountabilities

- [ ] Harden endpoints, utilise modern EDR and implement application whitelisting

Secure Cloud

Engaging the team to create a Business Continuity Plan (BCP) can help to reduce the financial, productivity and brand risk that results from a cyber-attack. Having a clearly documented and tested Disaster Recovery (DR) framework mitigates risk and minimises impact.

- [ ] Perform a detailed assessment of opportunities and risks
- [ ] Employ remote monitoring and management tools
- [ ] Implement cloud access management
- [ ] Audit cloud configurations to ensure compliance with best practice, policies and standards

Compliance and Documentation

Having the right structures and governance in place will ensure performance, productivity, and compliance for your business and ensure compliance.

- [ ] Create a security group to control and access documentation
- [ ] Identify and document different types of data/information stored in your environment, or cloud services
- [ ] Analyse risk and manage controls to ensure only admins can assess critical data
- [ ] Correctly document all relevant policies and procedures based on strict regulations
- [ ] Regularly review and test compliance requirements and actions, and document for audit
- [ ] Create a business continuity plan in consult with leadership and operational teams
- [ ] Evaluate obligations of third-party providers including data security, privacy, and management
- [ ] Evaluate contractual requirements
- [ ] Review and ensure compliance with regulatory demands

Change Management

Programs fall over when change programs are overlooked or poorly implemented. Prioritise change management in educating and enabling everyone, from internal stakeholders to end users.

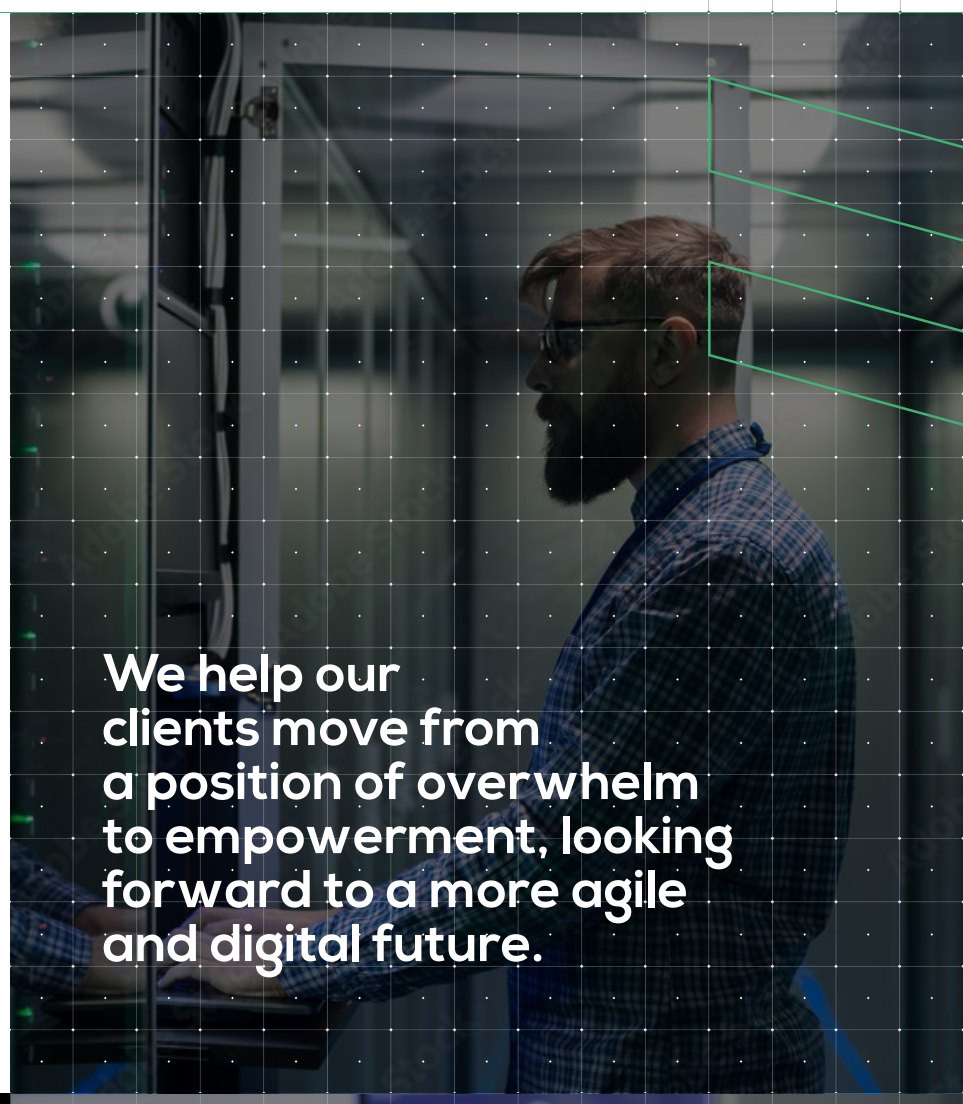
- ☐ Define the stages of change required in the process
- ☐ Keep all of your stakeholders informed
- ☐ Track all metrics associated with the change
- ☐ Report and reinforce security policies and training internally
- ☐ Review changes periodically to allow for enhancement due to the changing threat landscape

The Nexon advantage

Nexon Asia Pacific (Nexon) is an award-winning digital consulting and managed services partner for mid-market and government organisations across Australia. We have a uniquely broad suite of solutions to service clients who require end-to-end capabilities coupled with specialist expertise in security, cloud and digital solutions.

Our advanced solutions help clients to solve problems, address frictions and accelerate growth. Committed to the highest standards of responsiveness, competency and transparency, Nexon is built on a unique client care model that is fuelled by continuous feedback. With over 400 staff, we employ some of the country's most experienced consultants and empower teams to make decisions that accelerate change for client organisations.

As a certified and accredited local and state government provider, CREST and ISO-certified, Nexon partners with world-class technology vendors to deliver innovative solutions and service excellence.



nexon

Take the next step

For advice or support on any of these recommended actions and activities, get in touch, we're here to support your organisation and protect its assets, customers and people.

1300 800 000
enquiries@nexon.com.au
nexon.com.au

Follow **nexonap**