actlaw society

Procurement and Contract Management Cybersecurity

PRESENTED BY ANNIE HAGGAR AND AMANDA WESCOMBE

Cyber CG

actlawsociety

CYBER

About Cyber GC

Cyber GC is a specialist cybersecurity legal and consulting practice based in Australia, providing services all over world. We are dedicated to helping Australian businesses to prepare for, defend and recover from cyberattacks.

Cyber GC can bring specialist cybersecurity legal skills to complement your existing legal team, or to provide legal advice, strategy, and support to businesses and boards when they need it.

Annie Haggar

Founder and

Principal

Cyber GC

Annie is a multi-award-winning cybersecurity lawyer. She spent 12 years as legal counsel for one of the world's largest companies, including 6 years as global legal lead for its managed security business, now one of the largest cybersecurity companies in the world.

She has 20 years of experience advising government and private sector clients in technology law, enterprise security risk, procurement security considerations, global security regulation, and cybersecurity risk in mergers and acquisitions.

AUSTRALASIAN LAW AWARDS 2021

Lawyers Weekly AUSTRALIAN LAW AWARDS WINNER General Counsel of the Year 2021

Lawyers Weekly CORPORATE COUNSEL AWARDS WINNER TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS LAWYER OF THE YEAR 2021

Amanda Wescombe

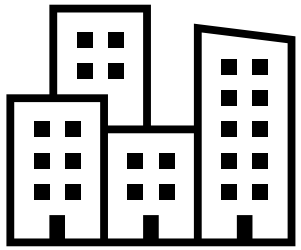
Special Counsel

Cyber GC

Amanda is a corporate and commercial lawyer, specialising in cybersecurity and technology.

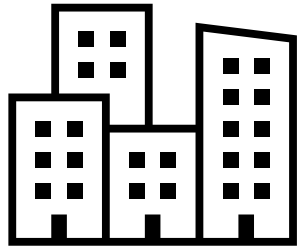
Having worked as in-house counsel for global brands, government, and in private practice, she has seen procurement and contract management from each of the sales and procurement side, across the spectrum of low-to-high risk and tiny-to-mega deal.

What is a supply chain?

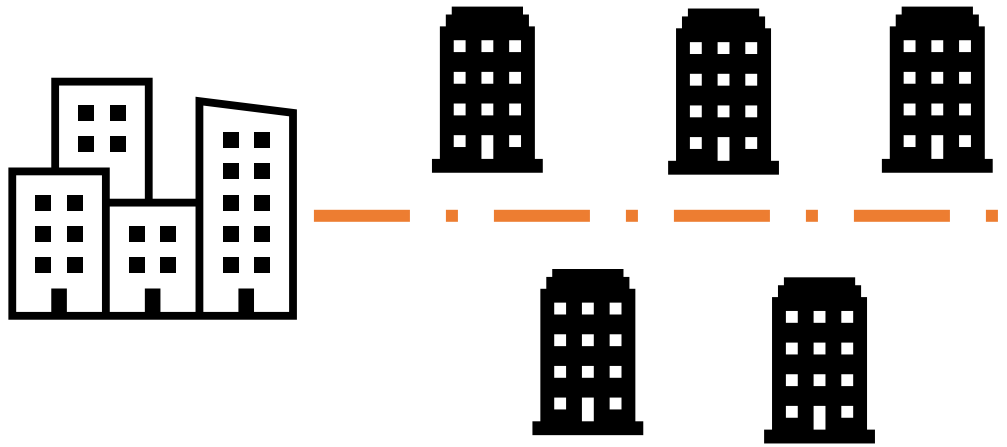


Menti


Organisation Supply Chain




Organisation Supply Chain


Customer/Client
Supply Chain

Why are ‘indirect’ or supply chain attacks an issue?

Prevalence

98%

of entities have suffered an attack via their supply chain (2023)

Impact

HWL EBSWORTH LAWYERS

“a total of 65 Australian Government entities have been impacted…

these agencies were clients of HWL Ebsworth and did not suffer a cyber incident themselves”

National Cyber Security Coordinator
Air Marshal Darren Goldie AM CSC

It doesn’t matter how secure you are, if you don’t secure your supply chain.

Sources: SecurityScorecard and SecurityWeek

Cybersecurity in Commonwealth Government Requirements

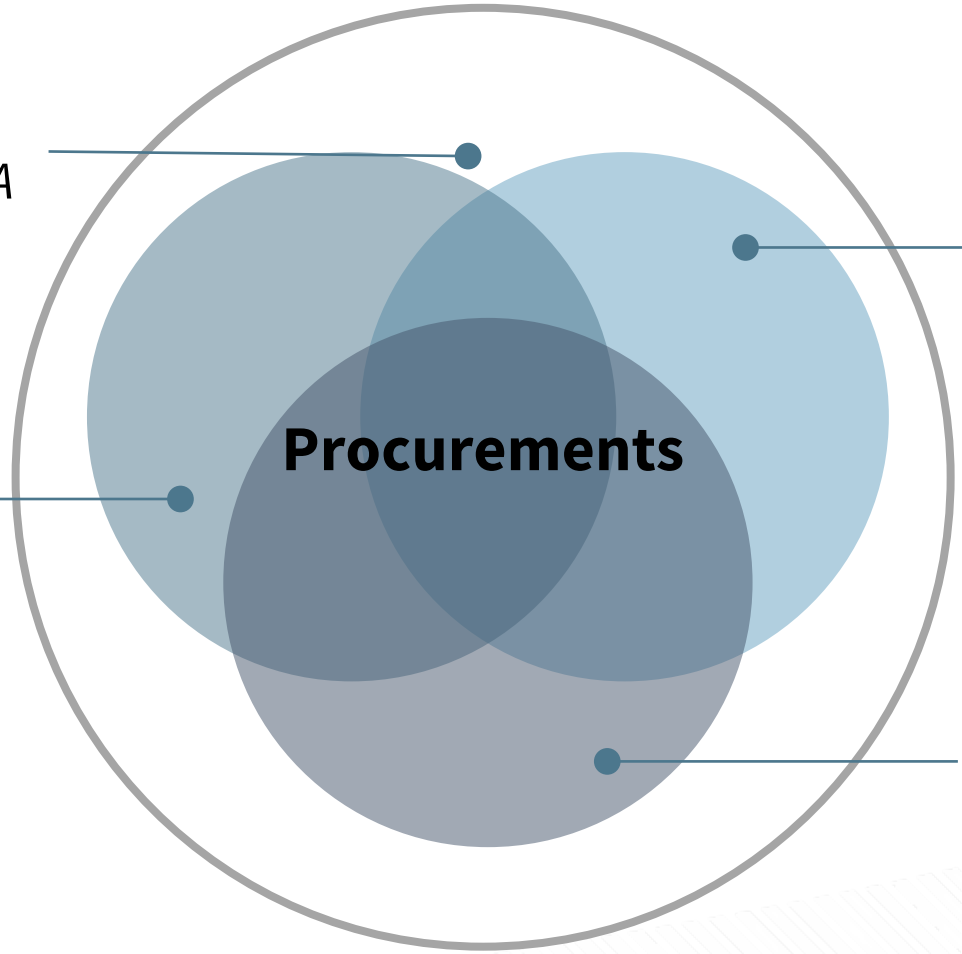
Public Governance, Performance and Accountability Act 2013 (PGPA Act)

Protective Security Policy Framework (PSPF)

<u>Policy 6 Security governance for contracted goods and service providers</u>

4 key areas –

1. Personnel Security
2. Information Security
3. Physical Security
4. Security Governance



Commonwealth Procurement Rules (CPRs)

Information Security Manual

actlawsociety

ANAO - Management of Cybersecurity Supply Chain Risks Report 2022

Three agencies audited

- Australian Federal Police
- Australian Taxation Office
- Department of Foreign Affairs and Trade

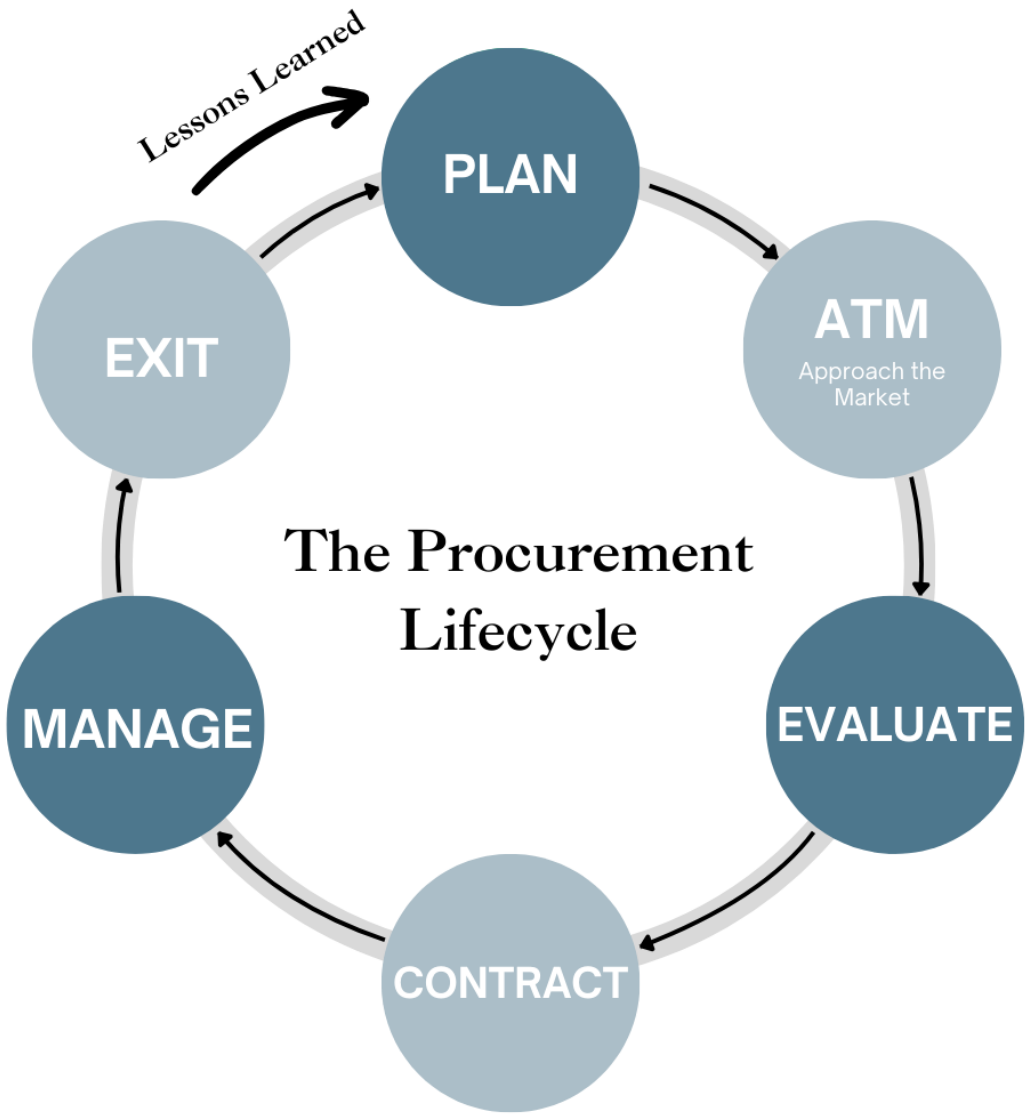
51%

Non-corporate Commonwealth agencies have not fully implemented the Protective Security Policy Framework (PSPF)

> *Contractors holding government information had a significant increase in malicious cyber activities*

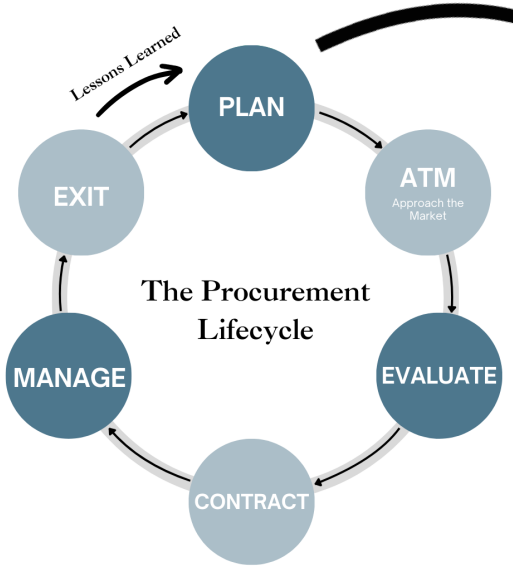
Arrangements for monitoring security controls for relevant PSPF requirements

Process Component	Entity Self-Assessment			ANAO Analysis		
	AFP	ATO	DFAT	AFP	ATO	DFAT
Contract terms and conditions for monitoring security controls	●	●	●	◑	◕	◑
Guidance and Support	●	●	●	◕	●	◑
Issue Management	●	●	●	◑	●	◑
Performance Reporting	●	●	●	◑	●	◑


Lessons Learned
PLAN
ATM
Approach the Market
EVALUATE
CONTRACT
MANAGE
EXIT
The Procurement Lifecycle

Menti

Menti



Plan

SECURITY RISK ASSESSMENT

1. Identify components
2. Assess nature of product/service, operational impact
3. List potential threats
4. Plan mitigations using policy, process, contract, technical and operational controls

PERSONNEL SECURITY ‘minimum access necessary’

- who has access to what
- how sensitive is the information they have access to?

PHYSICAL SECURITY ‘secure assets’

- assets: what, where
- access: what, how

INFORMATION SECURITY ‘protecting information’

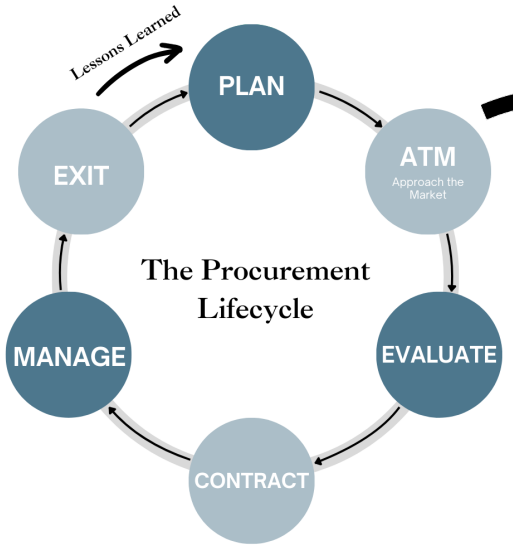
- data: what, where, sensitivity, value
- transfer: where from, where to

GOVERNANCE ‘control factors’

- suppliers: who, where, size, maturity, how
- internal: stakeholders

LAWYER’S ROLE

- Be confident in asking questions about whether the security has been considered
- Ask to see the risk assessment and look for security



Approach To Market

SECURITY RISK CONSIDERATIONS

1. What personnel details are being released with the ATM?
2. What vulnerabilities of the department are being disclosed that could be exploited?
3. What is being disclosed which, when pieced together with other information, could identify vulnerabilities?

PERSONNEL SECURITY

'minimum access necessary'

- procurement inbox v personal email address
- NDAs for supplier personnel accessing tender docs

PHYSICAL SECURITY

'secure assets'

- physical tender briefing (location, attendance, materials, security, confidentiality)
- assets: what, location
- access: what, how

INFORMATION SECURITY

'protecting information'

- data: describe but don't identify if possible
- transfer: describe but don't identify if possible
- access: data room?

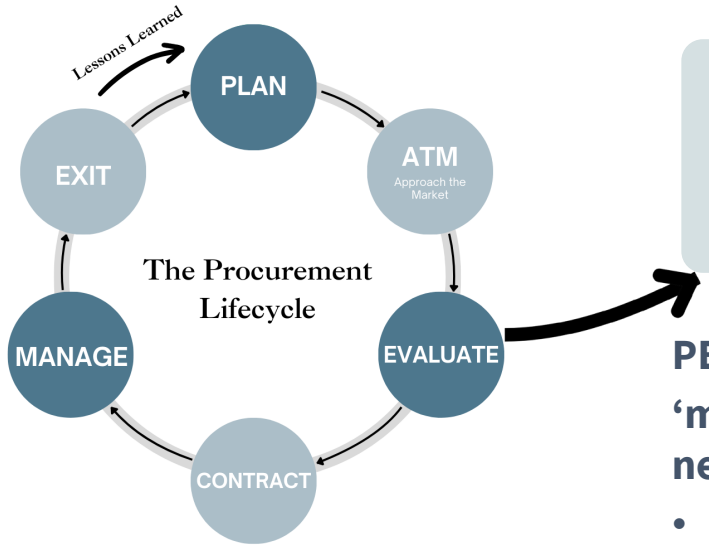
GOVERNANCE

'control factors'

- suppliers: who, where, size, maturity, how
- internal: stakeholders,
- limited ATM
- AusTender exemption?

LAWYER'S ROLE

- Assisting with NDA
- Question whether AusTender exemption is appropriate
- Review tender docs and ensure security is adequately addressed for the risk profile



Evaluate

SECURITY RISK EVALUATION

1. How is the security of the tenderer being evaluated?
2. How is the security of the solution being evaluated?
3. How are the security risks discussed at the plan stage included in the evaluation criteria?
4. How are the evaluated risks being included in the overall decision making?

PERSONNEL SECURITY

'minimum access necessary'

- who has access to what information in the evaluation team?
- NDAs
- Security clearances

PHYSICAL SECURITY

'secure assets'

- where are you evaluating
- offsite security

INFORMATION SECURITY

'protecting information'

- third party procurement tool security
- evaluation results storage
- data leakage

GOVERNANCE

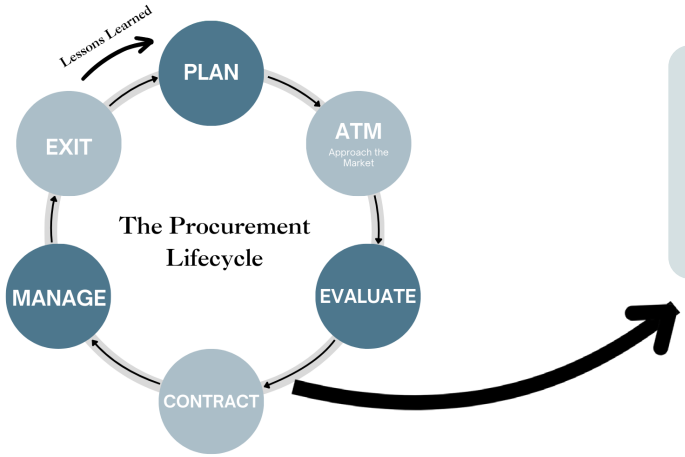
'control factors'

- security of the tenderer (system, past breaches, certifications)
- internal: stakeholders, conflict of interest 'insider threat'
- process and distribution of evaluation information

LAWYER'S ROLE

- Evaluating non-compliances with contract – including security clauses
- Feed in non-compliance risks to evaluation team

Menti



Contract

SECURITY IN THE CONTRACT

1. Security Requirements
2. PSPF checklist
3. Supplier security
4. Service/product specific
5. Service Levels/Service credits
6. Foreign access and control
7. Termination obligations
8. Cyber attack support and data breach support
9. Supply Chain visibility and control and flow through

PERSONNEL SECURITY

'minimum access necessary'

- background checks / security clearances
- Key Personnel
- location including support services
- personnel changes

PHYSICAL SECURITY

'secure assets'

- where is the work performed?
- do they need access to organization premises?
- are they escorted?

INFORMATION SECURITY

'protecting information'

- what data is held on vendor's systems?
- where is the data/system hosted
- what remote access is required?
- security of vendor's systems

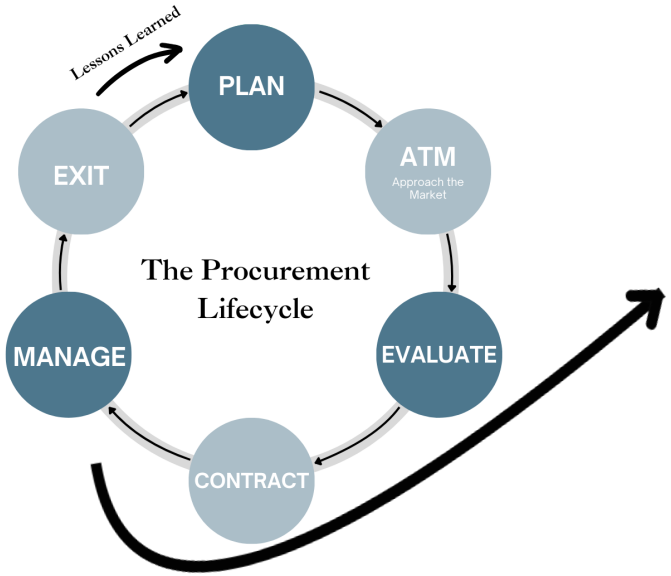
GOVERNANCE

'control factors'

- secure communication
- minimum information access
- performance management
- audit and reporting
- changes to security risks (internal and external)
- support during a breach

LAWYER'S ROLE

- Consider changes needed to WoGA
- Include appropriate security clauses for the risk profile in the draft contract (incl at ATM stage)
- Ask questions
- Negotiating to protect Cth security requirements



Manage

MANAGING SECURITY

1. Security briefings
2. Managing security service levels
3. Breach management
4. Security impact of service/product changes
5. Vendor Supply Chain audit/monitoring/flow through updates

PERSONNEL SECURITY

'minimum access necessary'

- roll on / roll off
- NDA
- clearance breaches
- change in circumstances

PHYSICAL SECURITY

'secure assets'

- changes in delivery location
- physical security briefings
- reporting physical security breaches

INFORMATION SECURITY

'protecting information'

- changes to hosting or support
- data breach reporting

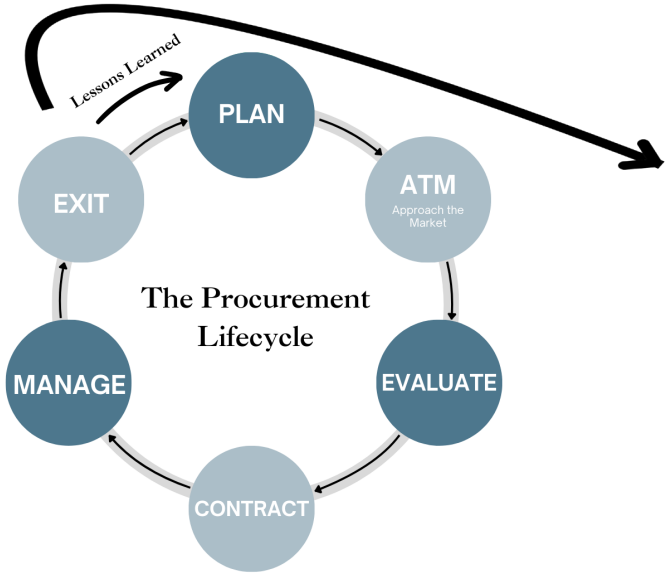
GOVERNANCE

'control factors'

- reporting on security compliance – and security qualified internal review
- audit and verification – 12 monthly security audit
- change in security profile – update contract
- breach management
- change in control and foreign government interest

LAWYER'S ROLE

- Assisting with managing breaches of security obligations
- Security impact of variations



Exit

PERSONNEL SECURITY

'minimum access necessary'

- roll off
- NDA – continuation of obligations post engagement
- exit security briefings
- key personnel handover

PHYSICAL SECURITY

'secure assets'

- return of assets and physical materials
- revoke access to premises

INFORMATION SECURITY

'protecting information'

- revoke access to systems
- handover of all data (in readable format)
- deletion of vendor copies (unless legally required) and certification

GOVERNANCE

'control factors'

- transition out plan and procedure
- handover
- post termination breach obligations (incl supply chain)
- ongoing security obligations (audit?)

SECURE EXIT

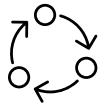
1. Briefings
2. Information handover
3. Asset handover
4. Lessons learned
5. Public Communications

LAWYER'S ROLE

- Advice on termination rights and outgoing security obligations
- Notification to vendor of ongoing security and confidentiality obligations
- Advice on rights /obligations to retain data
- Lessons learned

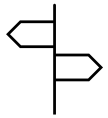
actlawsociety

Key points



Security should be considered for all procurements and at each stage of the procurement lifecycle

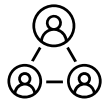
Legal has a role to play in managing security – even if you're not a cybersecurity lawyer



Don't be afraid to point out security issues if you spot them – security is everyone's job

Embed security 'by design' – not as a band-aid consideration at the last minute

Use the PSPF Policy 6 as a guide



Be curious – learn from each other and ask questions

Menti

Questions

CYBER GC

LEGAL - CONSULTING - BOARD

ANNIE HAGGAR | **AMANDA WESCOMBE**

PRINCIPAL | SPECIAL COUNSEL

annie@cybergc.au

amanda@cybergc.au

www.cybergc.au

actlaw society

ACT Law Society
Level 4, 1 Farrell Place, Canberra City ACT 2601
Phone 02 6274 0333 | memberassist@actlawsociety.asn.au

actlawsociety.asn.au