TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 305

December 2005

Identification processes in the higher education sector: risks and countermeasures

Russell G Smith

One of the most intractable crime problems that has arisen in the twenty-first century concerns the criminal misuse of identity – popularly known as identity fraud or identity theft. Computer technologies have enabled documents used to verify an individual's identity to be altered or counterfeited with ease, leading to a problem which, in 2001–02, was estimated to cost $1.1 billion in Australia alone (Cuganesan & Lacey 2003). The higher education sector is not immune from risks of identity-related fraud and other kinds of dishonest practices, and, as this paper demonstrates, risks are present throughout the sector – from enrolment of students, through the examination process, upon qualification, and during subsequent employment. Reducing the risks associated with identification of students and staff alike entails the employment of a wide range of strategies that need to be implemented uniformly across the entire sector. This paper analyses the nature of the problem and how government, business and individuals can share in the task of preventing identity thieves from enrolling and graduating dishonestly.

Toni Makkai
Director

In undergoing higher education, as well as in conducting many business transactions, people are required to establish who they are by providing evidence of unique identifying characteristics. It is usual to produce or disclose something that you *have* (tokens), something that you *know* (knowledge), something related to *who* you are (biometrics), or something indicating *where* you live (location). Of course there are others, such as the use of a person's name, and a variety of behavioural and psychological characteristics that can be used to identify people. Depending upon the degree of certainty with which one needs to establish one's identity, one or more of these methods may be relied upon. Often only one method will be used, and this will generally involve the disclosure of a document. Each has its own vulnerabilities and risks which are able to be exploited by those who want to act illegally.

In the past, identity was more easily verifiable as people conducted most of their transactions in person. With the advent of computers, however, documents can easily be fabricated and personal information obtained from electronic databases either by gaining access without authority, or by tricking unsuspecting users into disclosing their access codes and passwords. In higher education, examples of identity-related fraud and other dishonest practices exist in all aspects of the sector extending from enrolling as a student, undergoing examinations and submitting essays, commencing employment as a staff member, paying fees, receiving salaries, and using technology. There is a continuing need to identify both new students and staff with accuracy and the task for university administrators is considerable. In 2004, for example, 284,184 new students enrolled in Australian universities, 66,494 from overseas (Winchester & Lacey 2003: 194). In 2004, there were also 91,905 staff employed in Australian universities (Department of Education, Science and Training 2004). Evidence is needed of previous qualifications and/or eligibility to enrol for new students; previous employment and qualification

ISSN 0817-8542

ISBN 0 642 53894 8

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends & issues in crime and criminal justice series, visit the AIC web site at: http://www.aic.gov.au

Disclaimer:
This research paper does not necessarily reflect the policy position of the Australian Government

Project no. 0091

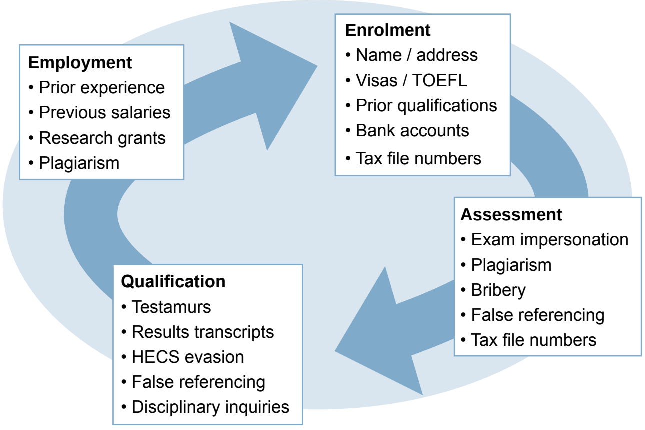
details for new staff; as well as identification necessary for conducting business transactions including payment of fees and receiving payments such as salaries.

In Australia, a wide range of documents may be used to establish identity. Included amongst them are student identity cards, 358,700 of which were issued by higher educational institutions in 2002–03 – many with rudimentary forms of security against alteration or counterfeiting. One recent study found that of the 16 state and territory Offices of Births, Deaths and Marriages, and driver licence issuing agencies, 15 of these organisations accepted student identity cards and/or statements of results as proof of a person's identity for purposes such as building access, computer access, library usage, public concessions, and examinations. Of these 15 organisations, two accepted tertiary sector documents and tokens without requiring further proof, one accepted photocopies through the mail, while 13 others accepted a combination of student cards, statements of results, or statements of enrolment with other documentation or tokens (Winchester & Lacey 2003: 194). If these are counterfeited or altered, they can form part of a chain of documents used to perpetrate a wide range of financial crimes. False student identity cards can be used (in conjunction with other documents) to obtain birth certificates, drivers' licences, passports and then to open bank accounts.

The regulatory environment

Identity-related fraud is governed by a wide range of rules in Australia. Numerous offences can be used to prosecute conduct involving misuse of identity. Each jurisdiction in Australia has a variety of offences that involve deception, dishonesty, and manipulation of documents. Some entail general crimes of dishonesty while others entail specific offences such as opening a bank account in a false name, or gaining unauthorised access to computers. In South Australia, the *Criminal Law Consolidation Act 1935* (SA) was amended in 2003 by the introduction of Part 5A that contains sections prescribing offences involving the assumption of a false identity, the use of personal identification information and the production and possession of prohibited material. Numerous offences also exist at the federal level including opening accounts in false names (s. 24 *Financial Transaction Reports Act 1988*), possessing a forged or falsified Australian passport (s. 9A *Passports Act 1938*), obtaining property or a financial advantage by deception (*Criminal Code* Division 134), fraudulent conduct (Division 135), forgery (Division 144) and falsification (Division 145). The *Financial Transaction Reports Act 1988* (Cth), also regulates the manner in which identity must be established when accounts with financial institutions are created (the so-called '100-point system').

Figure 1: Opportunity structure for identity-related fraud and dishonesty in higher education



In the higher education sector, various regulations are relevant to the control of dishonest and illegal practices including identity-related fraud. University disciplinary procedures, for example, can be used to deal with cases of staff or student misconduct which could include misuse of identity or fabrication of documents.

Risks of identity fraud in the higher education sector

In November 2003, Winchester and Lacey (2003: 195) reported the results of a review of all Australian university student enrolment and card issuing processes. This was conducted by obtaining information from public sources, in addition to conducting several focus group discussions with selected tertiary sector participants. It was found that although approximately 90 per cent of tertiary institutions request information on the applicant's name, date of birth, citizenship, and education record, few attempts are made to validate this information with external issuing authorities. Less than half of the institutions examined required the presentation of photographic identification when student cards were issued and there was some evidence of corruption within institutions in connection with the issuance of results transcripts and other documentation which could be used in connection with fraud. These less than satisfactory procedures create a range of opportunities for dishonesty to occur. Risks arise at all stages of academic life, as shown in Figure 1.

As with other types of identity-related fraud, the risk environment operates in a circular path: having enrolled using illegal identification, a person will be issued with a student identity card which can then be used as one of the documents needed to open a bank account. Having opened a bank account, a tax file number can be obtained which can be used in connection with loan fraud or avoiding a HECS liability. An improperly granted qualification could then be used to obtain an academic position, and research funding provided following the submission of dishonest information to the grant provider. A misleading curriculum vitae could then be used to seek promotion or a new academic position. The individual could then be authorised to enrol new students and to assess their work. Early identification of the risks at the beginning of such a cycle could minimise the risks of more elaborate and expensive deceptions taking place subsequently.

Fraud risks may arise for students, staff members and persons external to the institution, both in terms of commission as well as victimisation. The principal areas of concern are shown in Table 1 and illustrated by the following examples chosen from cases recently prosecuted in Australia and overseas.

Enrolment fraud

The initial entry point to the higher education sector can provide a number of opportunities for fraud. In one case, a student falsely claimed to have a Rabbinical Diploma from the Talmudical College in London when making an application for admission to study for the Degree of Bachelor of Arts at La Trobe University, in Melbourne. In his application he claimed that he held the diploma and produced a framed document testifying to this. On the basis of this document, he was given credit for four subjects. He undertook studies at La Trobe University and was awarded the Degree of Bachelor of Arts in 1989. An inquiry was subsequently undertaken by La Trobe University and an expert document examiner testified that the framed academic record produced was a forgery. In 1991, the Bachelor of Arts Degree was revoked by the University Council. The student lodged a petition against the revocation of his degree to the University Visitor, which was dismissed (*Re La Trobe University; ex parte Hazan* [1993] 1 VR 7). A subsequent appeal to the Supreme Court of Victoria was also dismissed (*Hazan v La Trobe University* (No 2) [1993] 1 VR 568).

Test of English as a Foreign Language (TOEFL) certificate fraud

Forgery of documents has also arisen in connection with overseas students qualifying for entry to Australia. In July 2003, a former mainland Chinese student was sentenced to nine months' periodic detention for forging TOEFL examination documents and other papers used to enable Chinese students to gain permanent residence in Australia. When police arrested him in Sydney, an illegal printing press was found with negatives of photocopied documents used to manufacture University of Sydney academic transcripts, logos for certificates of graduation, and TOEFL scorecards (Maslen 2003: 22).

Student identity card fraud

Crimes can also be facilitated through the counterfeiting of student identity cards. Sometimes, the forgery of cards will form part of a chain of activities which will lead to the commission of serious financial crime. In one case, between 1 June 1996 and 30 September 1996 two individuals created a false New South Wales interim driver's licence, a University of Technology Sydney student card with the offender's photograph, an Australian Tax Office receipt and an Energy Australia receipt using a computer and a printer. These false identification documents were then used to obtain credit cards which were used to withdraw more than $22,000 cash. One of the accused pleaded guilty and was sentenced to four years' imprisonment, which was reduced on appeal to two years' with a non-parole period of 18 months (*R. v Spiridonov* [1998] NSWSC 761).

Student loan fraud

Many opportunities also exist for the commission of fraud in connection with the financing of higher education. In the United States, one perpetrator defrauded the Department of Education of more than US$160,000 by submitting fraudulent student loan applications in the name of his mother and brother. He also submitted a further 2370 student loan applications requesting disbursement of approximately US$43.8 million. These applications were prepared using multiple fictitious identities that claimed attendance at various colleges in the United Kingdom (Jones-Davis 2004: 8–9).

Examination fraud

Identity fraud can also take place in connection with examination procedures. In a case which occurred in London in October 1980, a registered medical practitioner who held the qualifications MRCS England, LRCP London and FRCS England, impersonated his wife in the final examination for the Licentiate in Medicine and Surgery of the Society of Apothecaries of London and forged her signature beneath the declarations of identity made to the Court of Examiners. At a disciplinary hearing conducted by the General Medical Council, he was found guilty of serious professional misconduct and his name

Table 1: Higher education dishonesty and identity-related fraud risk matrix

	Student		Staff		External
	Victim	Offender	Victim	Offender	Offender
Entry					
Enrolment fraud		X			X
TOEFL certificate fraud		X			X
Student identity card fraud		X			X
In-Course					
Loan fraud		X			X
Examination fraud		X			X
Essay fraud		X			X
Database fraud	X	X	X	X	X
Qualification					
Qualifications fraud		X		X	X
Testamur fraud		X		X	X
HECS debt evasion		X		X	X
Employment (post-qualification)					
Employment application fraud				X	X
Administration fraud				X	
Research grant fraud				X	

X Indicates presence of risk

erased from the Register (General Medical Council 1981: 335).

Essay fraud

Many opportunities now exist for university students to cheat in connection with written essays and assignments. Researchers at Southern Cross University found that 350,000 essays were for sale on the Internet for between $50 and $140, while international studies have shown that approximately 10 per cent of university students' work was plagiarised. No evidence was found to support the perception that Asian students were more likely to cheat than others, although they are more likely to be caught because of the contrast between the stream of lucid English from the plagiarised work and their less-than-perfect English (Livingstone 2004: 9).

Database fraud

Because extensive databases of personal information concerning staff and students are maintained by higher educational institutions, they provide an attractive target for computer hackers and others who seek to obtain personal information for use in dishonest activities. On 3 January 2005, for example, it was discovered that electronic databases at George Mason University in Washington had been breached and personal information relating to more than 30,000 students obtained improperly. The hackers broke into a database used for issuing student identity cards which included names, photos, social security numbers, and campus ID numbers (McCullagh 2005).

Qualifications fraud

In Victoria, a law clerk who had been working in his brother's legal practice in Melbourne qualified for the degree of Bachelor of Laws of the University of Melbourne in 1980, but because of previous convictions, was ineligible to obtain admission to practise as a solicitor. Although only a law clerk, he represented to clients that he was qualified to practise as a solicitor; that he had gained admission to the law school of the University of Tasmania and had been Dux of the university; that he had obtained a degree in science from the University of Melbourne; and that when he had finished his law degree at the University of Melbourne, he had completed a master's degree and had obtained a scholarship to Harvard and completed a doctorate. Inquiries were conducted by the Law Institute of Victoria and it was found that the representations he had made were untrue (*Feldman v Law Institute of Victoria* [1998] 4 VR 32).

Testamur fraud

The Internet has provided an effective means of trading in counterfeit academic testamurs. In the United Kingdom, Peter Leon Quinn conducted an illegal business via the Internet from Liverpool for more than 20 years in which he sold degrees and certificates for hundreds of universities in the United Kingdom and elsewhere. Quinn's website listed 52 Australian tertiary institutions whose degrees were available for viewing on the website. The testamurs were good copies of the originals although some contained errors. They contained forged signatures, watermarks and seals and could be delivered within a few days. False certificates cost the equivalent of A$555 while false degrees and transcripts cost A$870. Orders could be placed by email with payment by cheque, electronic funds transfer, or postal order. The association of higher institutions in the United Kingdom obtained a number of injunctions against Quinn in February 2000, which required him to close down his website. He failed to comply with the court orders, and changed his website address regularly to avoid detection. In October 2004, he was sentenced by the High Court in London to twelve months' imprisonment, wholly suspended for two years, for contempt of court in failing to comply with injunctions (Liverpool Echo 2004: 4–5).

In another case, two American men conducted a fraudulent university, 'Trinity Southern University'. In a sting operation, officials from the Pennsylvania Attorney-General's Office paid US$398 for an MBA Degree which was awarded to a cat called 'Colby', including a transcript of results which indicated that the cat had earned a 3.5 grade point average (The Commercial Appeal 2004: A5).

HECS debt evasion

In 2004, Australian Taxation Office investigators discovered 355 people avoiding university fee HECS debt repayments amounting to $2 million through the use of false tax file numbers. The students had taken work under false names in order to avoid HECS repayments that took effect when their income exceeded $35,000 a year. Another 641 people with HECS debts had duplicate tax file numbers, although investigators did not have evidence they were used for fraudulent purposes (Wallace & Bissett 2004: 11).

Employment application fraud

Following graduation, individuals can also commit fraud when applying for employment by dishonestly claiming or over-stating their qualifications and previous experience. In one case, a Registered Division 2 Nurse in Victoria used the similar sounding name and qualification of a Division 1 Nurse to obtain employment with two health care organisations in Melbourne. She was charged with falsely claiming registration and was fined $42,000 and ordered to pay costs of more than $7400 (Berry 2004).

The recent inquiry into the registration and conduct of surgery undertaken at the Bundaberg Base Hospital by Dr Jayant Patel is an example of a doctor who had allegedly lied on his application for registration in Queensland by stating that his registration in any other jurisdiction was not subject to an undertaking, the imposition of condition, suspension or cancellation. The Bundaberg Hospital Commission of Inquiry (2005) has recently recommended that various charges be laid against Dr Patel, including charges of making false representations, fraud, negligence causing harm, and murder or unlawful killing.

Administration fraud

In July 2005, a former Associate Director at the School of International and Commercial Services at Victoria University in Melbourne was sentenced to 32 months' imprisonment with a non-parole period of 16 months after having pleaded guilty to five counts of conspiracy to defraud and one count of obtaining property by deception. He admitted having authorised false invoices from fictitious companies for work never undertaken amounting to $387,042 between December 1998 and March 2001. His two co-conspirators were each sentenced to periods of suspended imprisonment (Russell 2005).

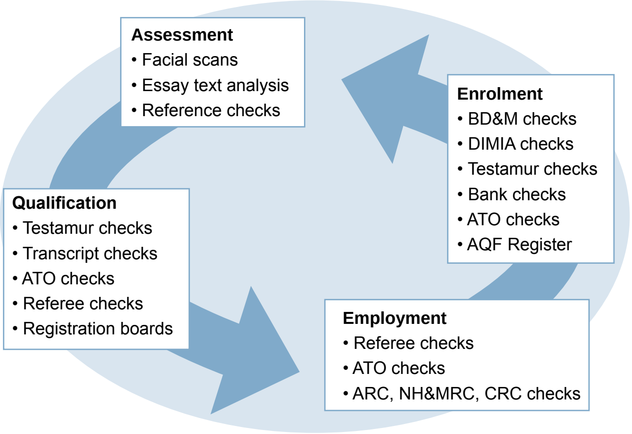
Research grant fraud

Finally, opportunities for fraud arise in connection with the application for, and use of, research funding. In 2003–04, for example, the Australian Federal Police completed an investigation into a medical researcher who had provided fraudulent information to the Australian Government in order to obtain research grants of $160,000 over four years (Australian Federal Police 2004: 40).

Key prevention strategies

How can these risks be minimised? At present, token-based identifiers and documentary evidence are the primary means of identifying individuals in the higher education sector – and are the most vulnerable to fraud. The key to fraud prevention lies in the effective use of verification of information with the issuing source. To combat each of the opportunities for identity-related fraud shown in Figure 1, a corresponding set of strategies can be employed, as shown in Figure 2. In this Figure, the direction of the arrows is reversed to indicate the need to establish verification procedures at the earliest stage of enrolment in the sector, so as to prevent opportunities being created in subsequent stages.

Figure 2: Verification procedures to reduce identity-related fraud in higher education



Ideally, the most stringent verification procedures should be applied to prospective students on enrolment, as this would help to ensure that further opportunities for fraud during assessment, qualification and employment are minimised. At present, the verification of information at enrolment is of varying degrees of thoroughness, although higher education institutions in Australia are beginning to explore the possibility of establishing systems to verify the qualifications which they grant and the authenticity of documents presented as evidence of having higher qualifications for student entrance requirements and staff appointment procedures.

In 2000, the National Protocols for Higher Education Approval Processes were established in Australia which provide criteria by which higher education providers deliver degree qualifications. These protocols have been further examined by the government in an attempt to ensure that only authorised providers are able to conduct higher education courses (Department of Education, Science and Training 2005). Previously, numerous organisations sought to provide qualifications without registration. Brown (2004) found that between 1999 and 2004, more than 27 unauthorised providers of higher education sought to deliver their programs to Australian students, or use Australia as brand leverage for their programs. It is now possible to check if providers are registered on the Australian Qualifications Framework Register, which provides a current listing of authorised providers (see http://www.aqf.edu.au/register.htm).

In relation to document security, RMIT University in Vietnam has begun using polymer banknote technology in order to minimise fraudulent alterations on issued transcripts and testamurs (Overland 2004). Polymer technologies are also being used by Monash University and the University of Melbourne to enhance the security of their academic records (Rood 2005).

A centralised authentication system for conferred qualifications is also currently being trialled in Queensland. QualSearch (http://www.qualsearch.com.au/) is an online verification system developed by the Queensland Tertiary Admissions Centre and enables a select range of Queensland institutions and members of the Recruitment and Consulting Services Association of Australia to carry out verification checks on a range of qualifications (Brown 2003). Ideally, QualSearch could be expanded to include all forms of qualifications issued by higher education institutions as well as professional licensing authorities and associations.

In another recent development, the New England Credit Union is using iris recognition systems in its branches and on its network to eliminate the fraudulent use of credit cards and accounts by students, and also to speed-up transaction time for customers (Sampson 2005). It is likely that such biometric solutions to user authentication will expand greatly in the years ahead.

Finally, various strategies can be used to reduce plagiarism, including the substitution of examinations for assignments and by designing assignments that are extremely specific to the particular students and the contexts in which subjects are taught, thus requiring research that cannot easily be drawn from the Internet (Livingstone 2004: 9).

Privacy issues

Because computers are able to track personal information so readily, it is important for any information about an individual's identity to be kept securely and used only for authorised purposes. Any system in which personal information is held in databases for the purpose of establishing verification checks to be undertaken – by government, or by private sector organisations – needs to comply with these strict legislative privacy protections so that personal information cannot be used for improper or unauthorised purposes. Individuals also need to be able to check the accuracy of the information that is kept and to obtain redress if that information is incorrect or misused in any way. Systems of accountability need to be established to protect information from unauthorised disclosure.

Conclusions

Accompanying the ever-expanding higher education sector is an ever-increasing problem of misuse of personal information. The drivers of identity-related fraud and other dishonest practices in this sector include the large financial implications which higher education now carries, the fluidity of the student market in which overseas education is now common, and the ready availability of technologies which can be used to fabricate or alter documents used to establish identity and qualifications, or to permit access to personal information stored electronically.

Ironically, it is these same factors which can be used to address the problem. Computers can provide an efficient and speedy means of verifying the authenticity of information which can enhance the processes of enrolment and qualification. A market is also being created for information brokers to carry out background checks on applicants for courses and jobs. The challenge for the future lies in ensuring that the data being verified are accurate and that information is not provided for unauthorised or improper purposes. Unless carefully monitored, an effective crime reduction system could, itself, create opportunities for identity thieves who are seeking legitimate sources of information which they can misuse.

Acknowledgments

The author is grateful to Mr George Brown, Director, HigherEd Consulting (Australasia) Pty Ltd, for providing invaluable information for this paper, and to Ms Kristi Cooper, intern at the AIC, for conducting background research.

References

Links were checked and operational at 19 October 2005.

Australian Federal Police 2004. *Annual report 2003–04*. Canberra: Australian Federal Police

Berry J 2004. Nurse gets record fine for registration deceptions. *The Age* 23 December: 5

Brown G 2003. Degrees of doubt: legitimate, real and fake qualifications in a global market. http://www.higheredconsulting.com.au/

Brown G M 2004. Protecting Australia's higher education system: a proactive versus reactive approach in review 1999–2004. Australian Universities Quality Forum *Quality in a time of change*. Adelaide: Australian Universities Quality Agency: 89–98

Bundaberg Hospital Commission of Inquiry 2005. *Interim report*. http://www.bhci.qld.gov.au/

Cuganesan S & Lacey D 2003. *Identity fraud in Australia: an evaluation of its nature, cost and extent*. Sydney: SIRCA

Department of Education, Science and Training 2004. *Education statistics 2004*. Canberra: DEST. http://www.dest.gov.au/sectors/higher_education/publications_resources/statistics/documents/students_2004_first_half_year.htm

Department of Education, Science and Training 2005. *Building university diversity: future approval and accreditation processes for Australian education*. Canberra: DEST. http://www.dest.gov.au/highered/pubs/building_diversity/default.htm

General Medical Council 1981. *Minutes of the proceedings of the Professional Conduct Committee*, 10 March, vol CXVIII: 130–131

Jones-Davis S 2004. Identity theft within federal student aid programs. *FBI law enforcement bulletin* vol 73 no 3: 8–9

Liverpool Echo 2004. Suspended sentence for degree fraudster. 28 October: 4–5

Livingstone T 2004. Uni answers out there for cheats. *Courier mail* 29 April: 9

Maslen G 2003. Students of crime. *Bulletin* vol 121 no 6384: 22

McCullagh D 2005. University suffers massive ID data theft. *CNET news* 11 January. http://news.zdnet.co.uk/internet/security/0,39020375,39183592,00.htm

Overland M A 2004. Institution prints its diplomas on paper typically used in bank notes. *Chronicle of higher education* vol 51 no 12: A37

Russell M 2005. Scholar jailed over uni scam. *The Age* 24 July: 4

Sampson G 2005. Detecting fraud and corruption by optimizing new technology and innovation. Paper to IIR public sector fraud and corruption conference. Canberra: 28 July

The Commercial Appeal 2004. MBA for cat busts fake degree sales.11 December: A5

Wallace M & Bissett K 2004. An education in fee evasion *Daily Telegraph*. 1 November: 11

Winchester D & Lacey D 2003. Identity fraud in Australia: implications for higher sector integrity in Marsden H Hicks M & Bundy A (eds) *Educational integrity: plagiarism and other perplexities* Adelaide: University of South Australia: 192–196

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology

General editor, Trends & issues in crime and criminal justice series:
Dr Toni Makkai, Director,
Australian Institute of Criminology,
GPO Box 2944 Canberra ACT 2601
Note: Trends & issues in crime and criminal justice are peer reviewed

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*