



Your partner
in progress

신뢰할 수 있는 AI 도입을 위한 가이드





“큰 힘에는 큰 책임이 따른다”는 말은 AI 분야에서 그 어느 때보다도 더욱 적절합니다. AI는 더 나은 의사결정을 내리고, 프로세스를 개선하며, 제품을 그 어느 때보다 빠르게 발전시킬 수 있도록 돕는 강력한 도구입니다. 하지만 잘 아시다시피 AI에는 다양한 위험도 존재합니다.

따라서 AI를 윤리적이고 공정하며 개인정보를 존중하는 방식으로, 그리고 안전하게 활용하기 위해서는 적절한 관리 체계(Guardrails)가 필수적입니다.

이러한 이유로 BSI는 **AI Foundation Framework**를 개발했습니다. 이를 통해 조직이 AI 도입을 효과적으로 관리하고, AI 활용에 대한 신뢰를 구축할 수 있도록 지원합니다.

David Mudd

BSI Global Head of Digital Trust Assurance

AI 시대의 화폐는 신뢰입니다

AI는 조직이 혁신을 이루고 가치를 제공하는 방식을 변화시키고 있습니다.

한때 새롭고 실험적인 기술로 여겨졌던 AI는 이제 일상적인 비즈니스의 일부가 되고 있으며, 오늘 내리는 결정은 장기적으로 긍정적이거나 부정적인 영향을 미치게 됩니다.

이해관계자의 기대, 규제, 표준이 지속적으로 변화하는 상황에서 조직은 AI 도입을 통제할 수 있어야 합니다. 또한 신뢰할 수 있는 검증(Assurance)을 제공할 수 있는 실질적인 방법이 필요합니다.

AI Foundation Framework는 이러한 요구를 충족합니다.

이 프레임워크는 현재 AI 성숙도 수준과 관계없이 조직이 AI 도입을 체계적으로 관리할 수 있도록 명확한 방법을 제공합니다. 복잡한 과제를 모듈 단위로 나누어 가장 중요한 영역부터 시작하고, 점진적으로 역량을 강화할 수 있습니다.

프레임워크를 활용하면 AI 리스크를 평가하고, 거버넌스를 강화하며, 개인정보 보호와 보안을 유지하는 윤리적 AI 운영을 입증할 수 있습니다. 또한 체계적인 교육, 자가진단(Self-assessment), 독립적인 검증 과정을 통해 책임 있는 AI 도입 수준을 측정하고 증명할 수 있습니다.

귀사의 AI 도입 여정에
가장 적합한 모듈을 찾아보세요.



AI Foundation Framework란?

AI Foundation Framework는 조직이 AI 도입에 대한 통제력과 책임성을 확보할 수 있도록 지원합니다.
이 프레임워크는 국제적으로 인정받는 표준을 기반으로 한 모듈형 검증 체계(Modular Verification Scheme)이며, 조직의 우선순위와 AI 성숙도 수준에 맞춰 적용할 수 있습니다.

이를 통해 조직은 단계적으로 역량(Capability), 자신감(Confidence), 그리고 신뢰(Trust)를 구축할 수 있습니다.

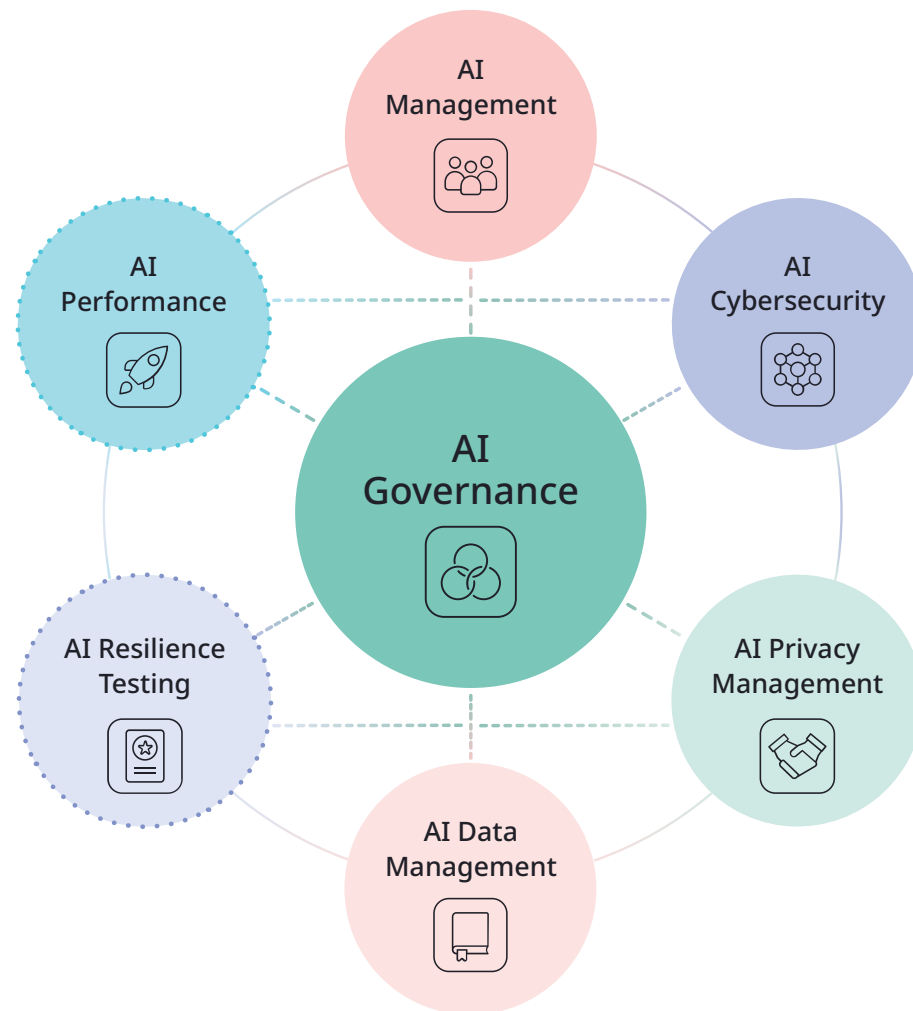
모듈형 프레임워크의 장점

- **독립성(Independence)**
: 국제적으로 인정받는 표준 기반
- **유연성(Flexibility)**
: 조직 목표에 맞는 모듈 선택 가능
- **가이드(Guidance)**
: 단계별 지원 제공
- **발전성(Progression)**
: 목표 성숙도 수준 설정 가능
- **증빙(Proof)**
: BSI Mark of Trust 획득을 통한 신뢰 입증

프레임워크 구성

- **AI 관리 역량에 대한 신뢰를 구축하는 5개의 모듈**
교육, 자가진단, 독립 검증 과정을 통해 조직의 AI 관리체계 성숙도를 평가하고 지속적으로 향상할 수 있도록 지원합니다.
- **AI 성능 및 복원력을 검증하는 2개의 모듈**
기술 표준을 기반으로 AI 시스템의 실제 성능과 복원력을 평가하여 강점과 개선이 필요한 영역을 명확하게 확인할 수 있도록 지원합니다.

각 모듈을 클릭하여 자세한 내용을 확인해 보세요.





AI 거버넌스

AI를 적절히 관리하고 있다는 확신을 제공하는 거버넌스 및 리스크 관리 모듈

주요 평가 영역: AI 사용 정책, 책임성과 의사결정 체계, 리스크 평가, 성과 모니터링 등

1. 교육

- 3~4시간 분량의 온디맨드 이러닝 교육
- 표준, 영역, 통제 항목 개요
- 자가진단 도구 소개
- 성숙도 수준 및 점수 체계

2. 자가진단

- 교육 과정 중 시작
- 원하는 속도로 진행
- 반복 수행 가능

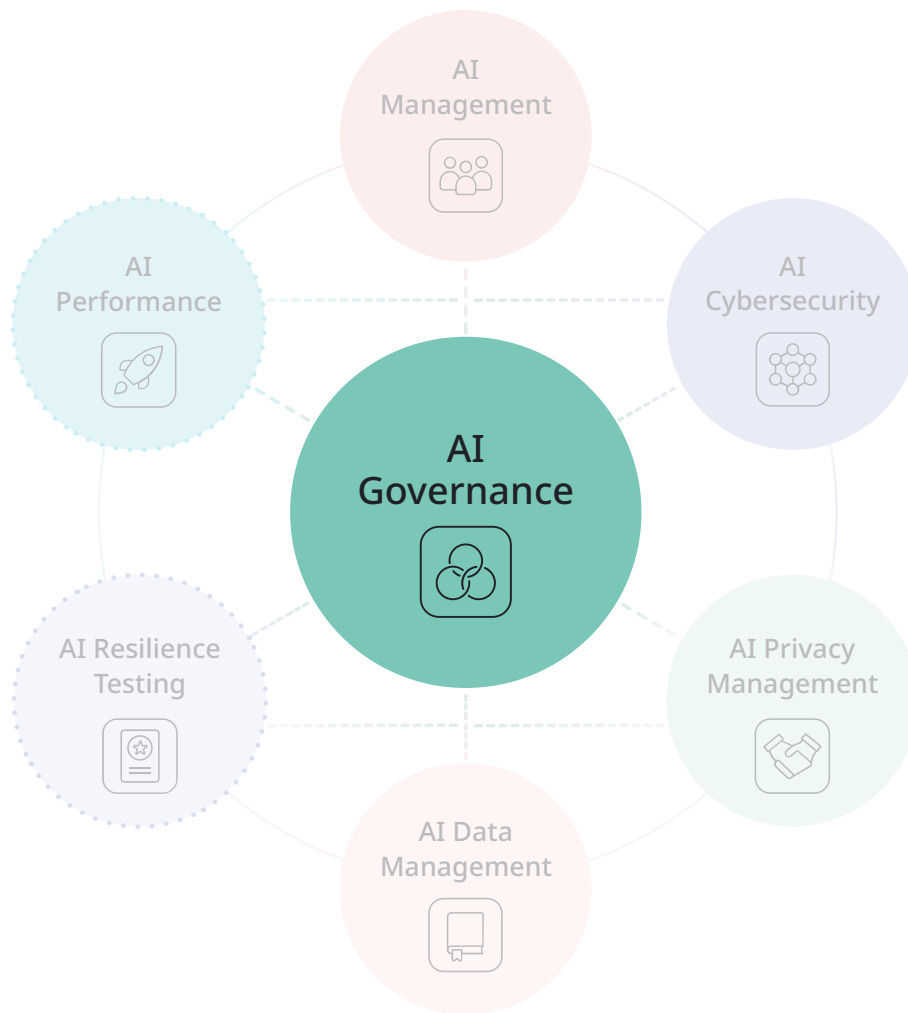
3. 검증

- 참조 표준
 - > ISO 38507 (IT 거버넌스)
 - > ISO 23894 (AI 리스크 관리)
 - > NIST AI Risk Management Framework
- AI 거버넌스 영역 3개
- 통제 항목 8개

4. 결과

- 검증 보고서
- 성숙도 평가 결과
- BSI 트러스트 마크

각 모듈을 클릭하여 자세한 내용을 확인해 보세요.





AI 경영시스템

AI 관리체계가 실제로 얼마나 효과적으로 운영되고 있는지 평가하고 개선점을 도출

주요 평가 영역: 거버넌스 및 감독, AI 생애주기 관리, MLOps 통제, 품질, 안전성, 강건성(Robustness)

1. 교육

- 3~4시간 분량의 온디맨드 이러닝 교육
- 관련 표준, 평가 영역 및 통제 항목에 대한 이해
- 자가진단 도구 활용 방법 안내
- 성숙도 수준 및 평가 방식 소개

2. 자가진단

- 교육 과정에서 시작, 교육 과정에서 시작, 원하는 일정에 따라 자율적으로 수행 가능

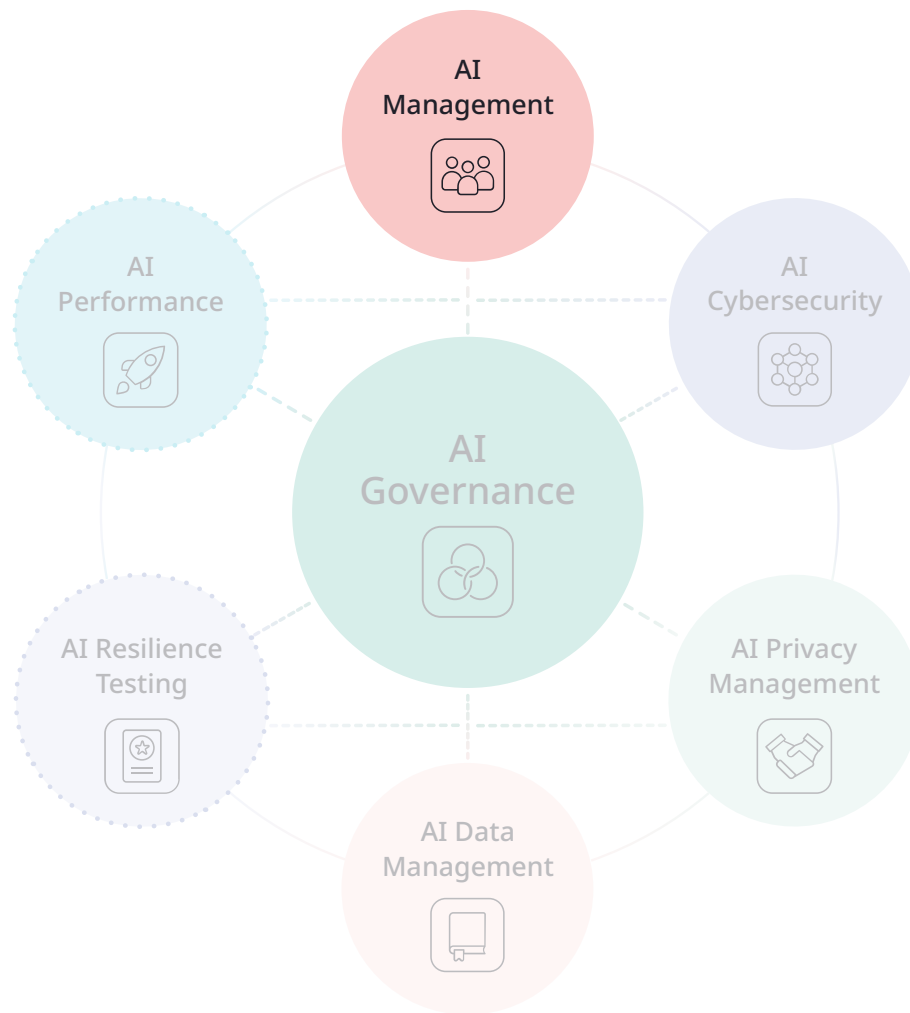
3. 검증

- 참조 표준
>ISO/IEC 42001 (AI Management)
>NIST Risk Management Framework
- AI 관리 영역 7개 평가
- 33개의 통제 항목 검토

4. 결과

- 검증 보고서 제공
- AI 관리체계 성숙도 평가 결과 제공
- BSI 트러스트 마크

각 모듈을 클릭하여 자세한 내용을 확인해 보세요.





AI 사이버보안 관리

AI 관련 사이버보안 리스크를 식별하고 대응

주요 평가 영역: 데이터 보안 및 보호, 데이터 포이즈닝(Data Poisoning), 모니터링, 탐지 및 포렌식

1. 교육

- 3~4시간 분량의 온디맨드 이러닝 교육
- 관련 표준, 평가 영역 및 통제 항목 소개
- 자가진단 도구 안내
- 성숙도 수준 및 평가 체계 설명

2. 자가진단

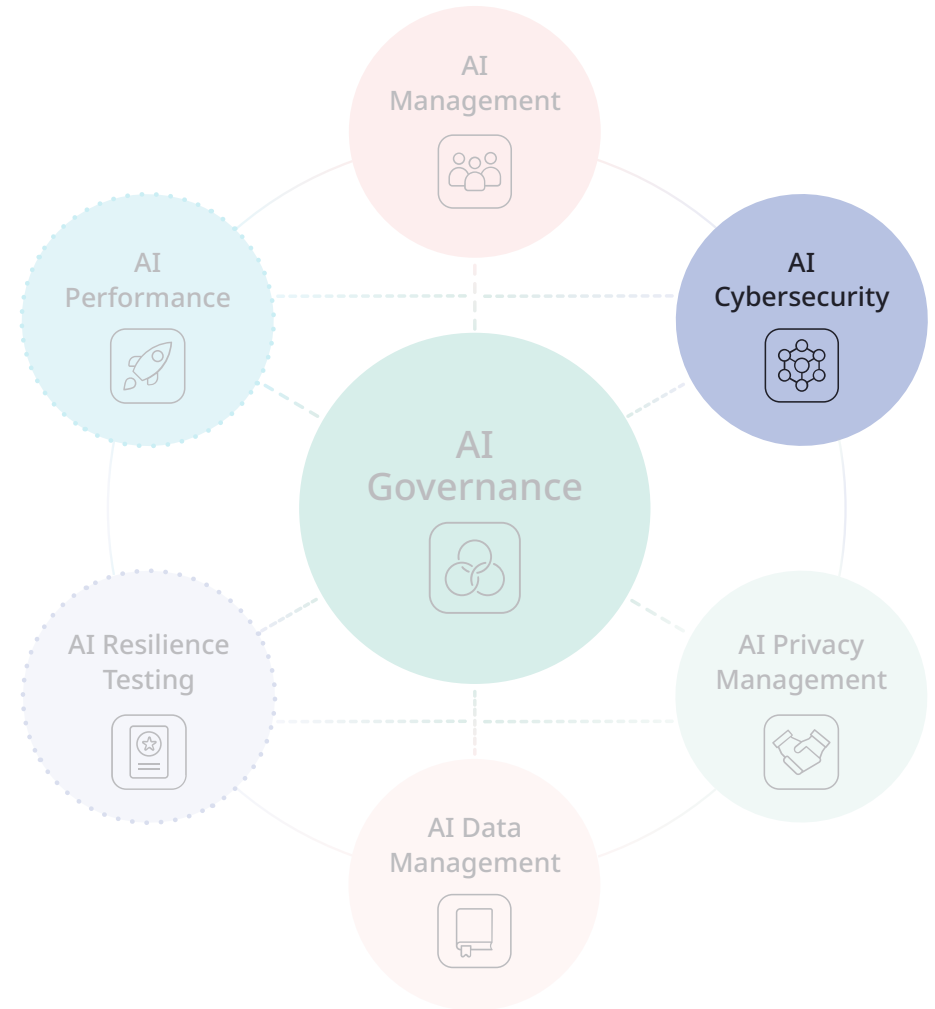
- 교육 과정에서 시작, 조직의 상황에 맞춰 자유롭게 수행 가능

3. 검증

- 참조 표준
 - >ISO/IEC 27001 (Information Security)
 - >ISO/IEC 42001 (AI Management)
 - >NIST Cybersecurity Framework
- 16개 사이버보안 영역 평가
- 90개 이상의 통제 항목 검토

4. 결과

- 검증 보고서 제공
- 사이버보안 관리체계 성숙도 평가 결과 제공
- BSI 트러스트 마크





AI 개인정보보호 관리

개인정보를 보호하여 프라이버시 우려를 해소

주요 평가 영역: 개인정보 식별 및 유출 방지, 라이프사이클 관리, 적법성, 개인정보 보호, 투명성, 모니터링

1. 교육

- 3~4시간 분량의 온디맨드 이러닝 교육
- 관련 표준, 평가 영역 및 통제 항목 소개
- 자가진단 도구 안내
- 성숙도 수준 및 평가 체계 설명

2. 자가진단

- 교육 과정에서 시작, 원하는 일정에 따라 자율적으로 수행 가능

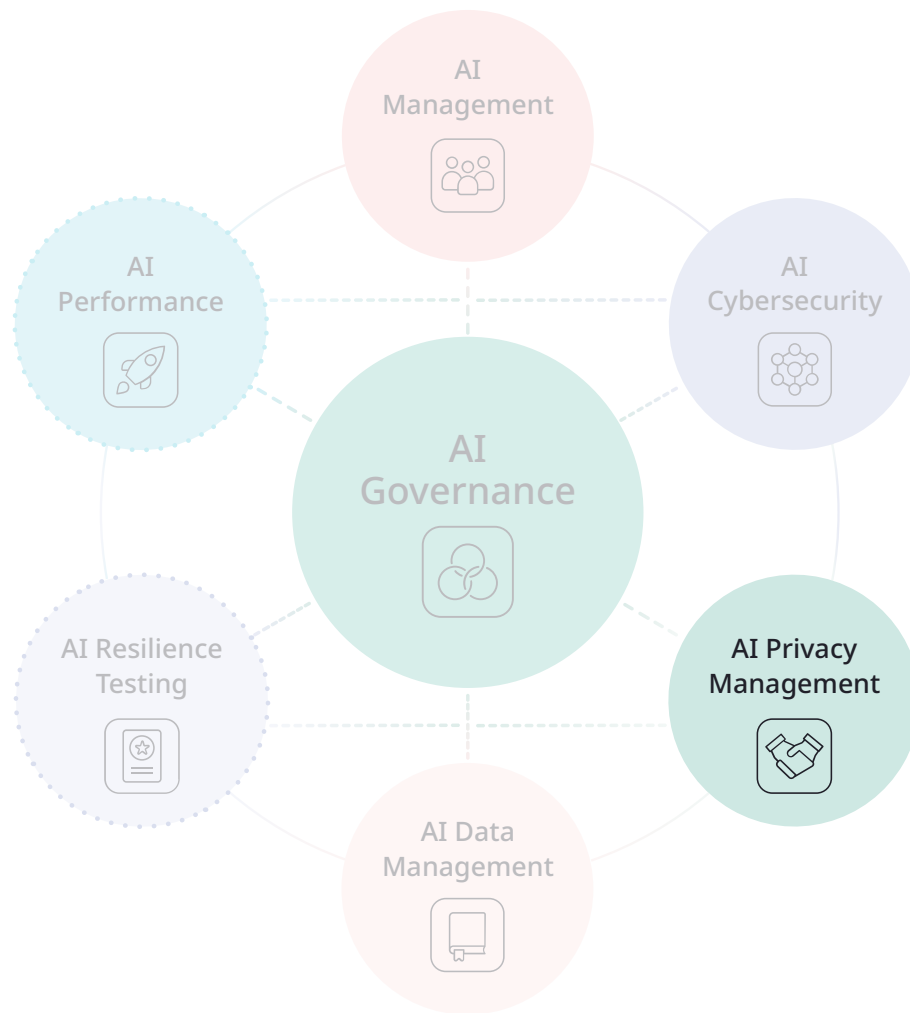
3. 검증

- 참조 표준
 - > ISO/IEC 27701 (Privacy Management)
 - > NIST Privacy Framework
- 23개 개인정보보호 영역 평가
- 38개의 통제 항목 검토

4. 결과

- 검증 보고서 제공
- 개인정보보호 관리체계 성숙도 평가 결과 제공
- BSI 트러스트 마크

각 모듈을 클릭하여 자세한 내용을 확인해 보세요.





AI 데이터 관리

신뢰할 수 있고 반복 가능한 결과를 제공하기 위한 데이터 품질 확보

주요 평가 영역: 데이터 라이프사이클, 데이터 품질 관리, 분석 및 머신러닝을 위한 데이터 품질

1. 교육

- 3~4시간 분량의 온디맨드 이러닝 교육
- 관련 표준, 평가 영역 및 통제 항목 소개
- 자가진단 도구 안내
- 성숙도 수준 및 평가 방식 설명

2. 자가진단

- 교육 과정에서 시작, 원하는 일정애 따라 자율적으로 수행 가능

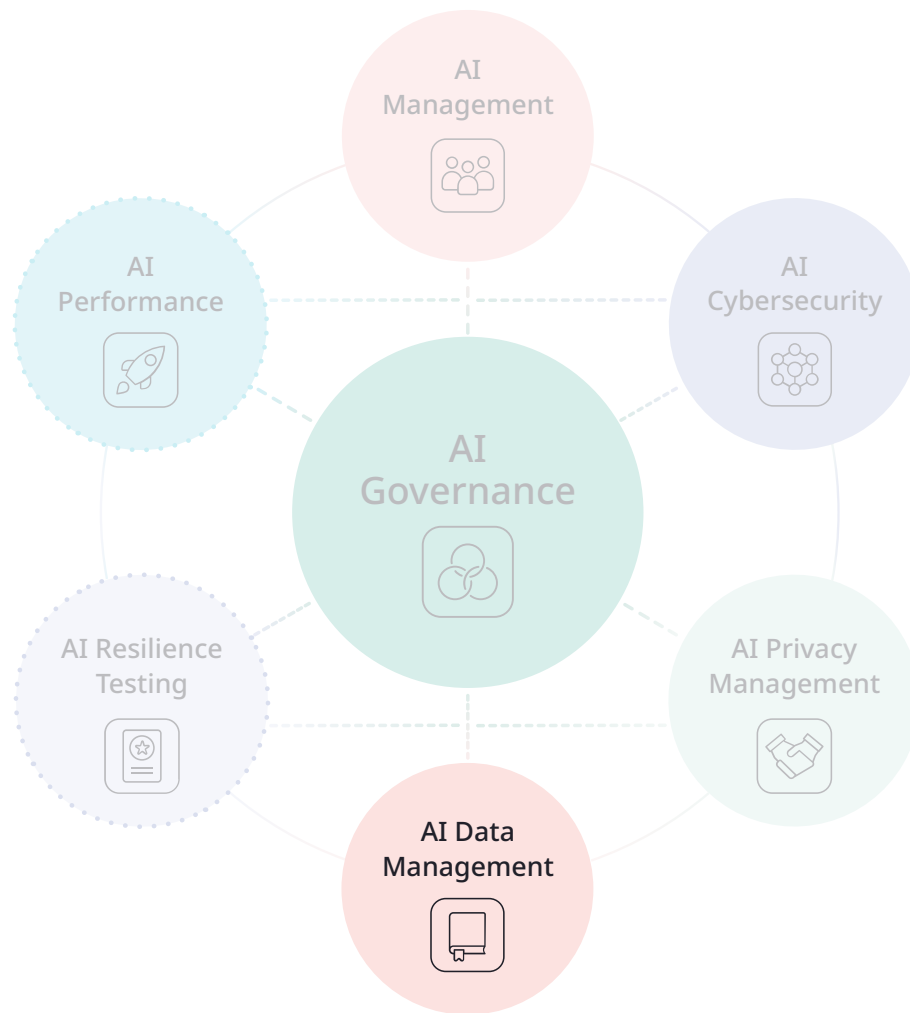
3. 검증

- 참조 표준
> ISO 38505 (Data Governance) >
ISO 5259-3 (Data Quality)
- 8개 AI 데이터 관리 영역 평가
- 81개의 통제 항목 검토

4. 결과

- 검증 보고서 제공
- 데이터 관리체계 성숙도 평가 결과 제공
- BSI 트러스트 마크

각 모듈을 클릭하여 자세한 내용을 확인해 보세요.





AI 복원력 테스트

AI 시스템을 실제로 검증하여 취약점을 식별하고, 보다 강력한 복원력을 확보할 수 있도록 지원합니다.

주요 평가 영역: 복원력 테스트(Resilience Testing), 레드팀 평가(Red Teaming), 침투테스트(Penetration Testing), 취약점 및 공격 시뮬레이션(Vulnerability & Attack Simulation)

1. 교육

- AI 복원력 개요
- 복원력 테스트 수행을 위한 준비 사항 안내

2. 자가진단

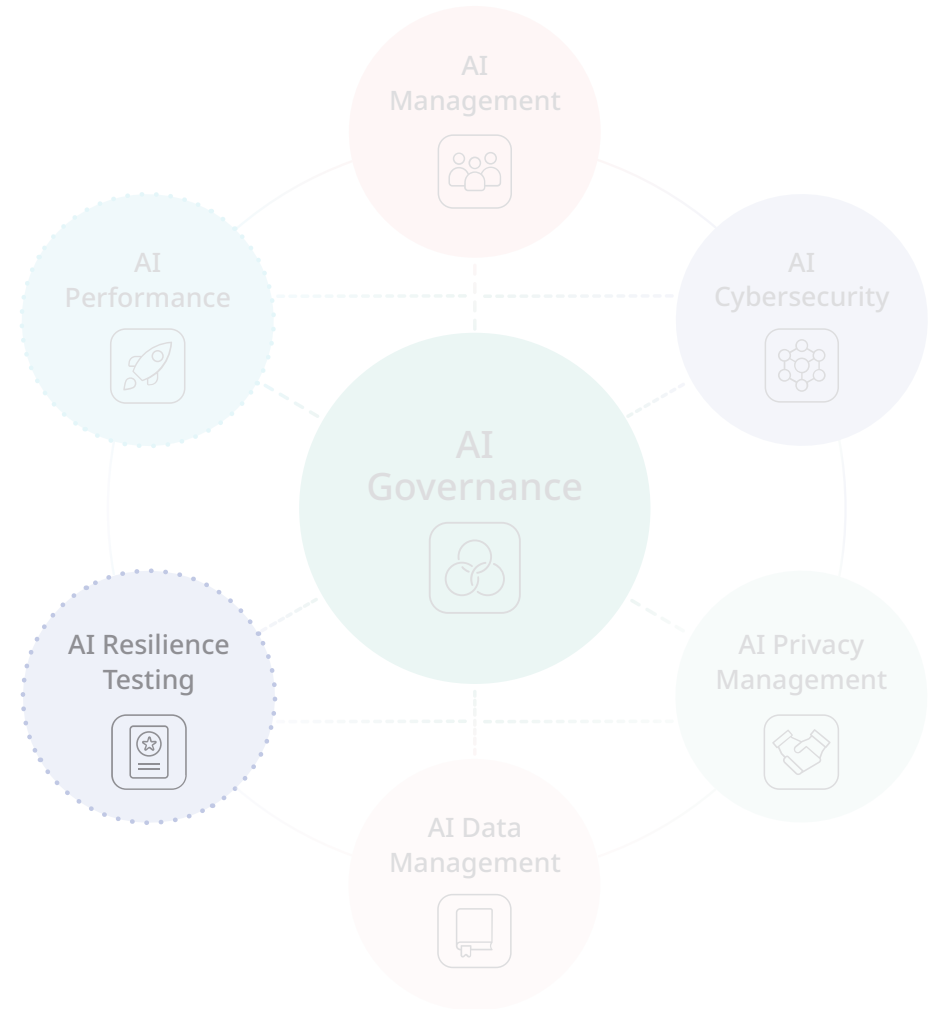
- 본 모듈은 자가진단을 포함하지 않습니다.

3. 테스트

- 레드팀 평가 수행
- 침투 테스트 수행
- 취약점 및 공격 시뮬레이션 수행

4. 결과

- AI 복원력 테스트 보고서 제공
- 확인서 발급
- BSI 트러스트 마크





AI 성능 테스트

AI 성능, 편향성(Bias), 강건성(Robustness)에 대한 신뢰성 있는 검증 제공

주요 평가 영역: AI 모델 테스트, 데이터셋 성능, 회귀 분석, 분류, 객체 탐지, 세분화(Segmentation), 식별 및 검증

1. 교육

- 본 모듈에는 별도의 교육 과정이 포함되지 않습니다.
- 필요 시 다음 관련 교육 과정을 통해 역량을 강화할 수 있습니다.
 - > ISO/IEC TS 4213 (Assessment of machine learning: 머신러닝 평가)
 - > ISO/IEC TR 24027 (Bias in AI systems & AI aided decision-making: AI 시스템 및 AI 기반 의사결정의 편향성)
 - > ISO/IEC TR 24029-1 (Robustness of Neural Networks: 신경망의 강건성)

2. 자가진단

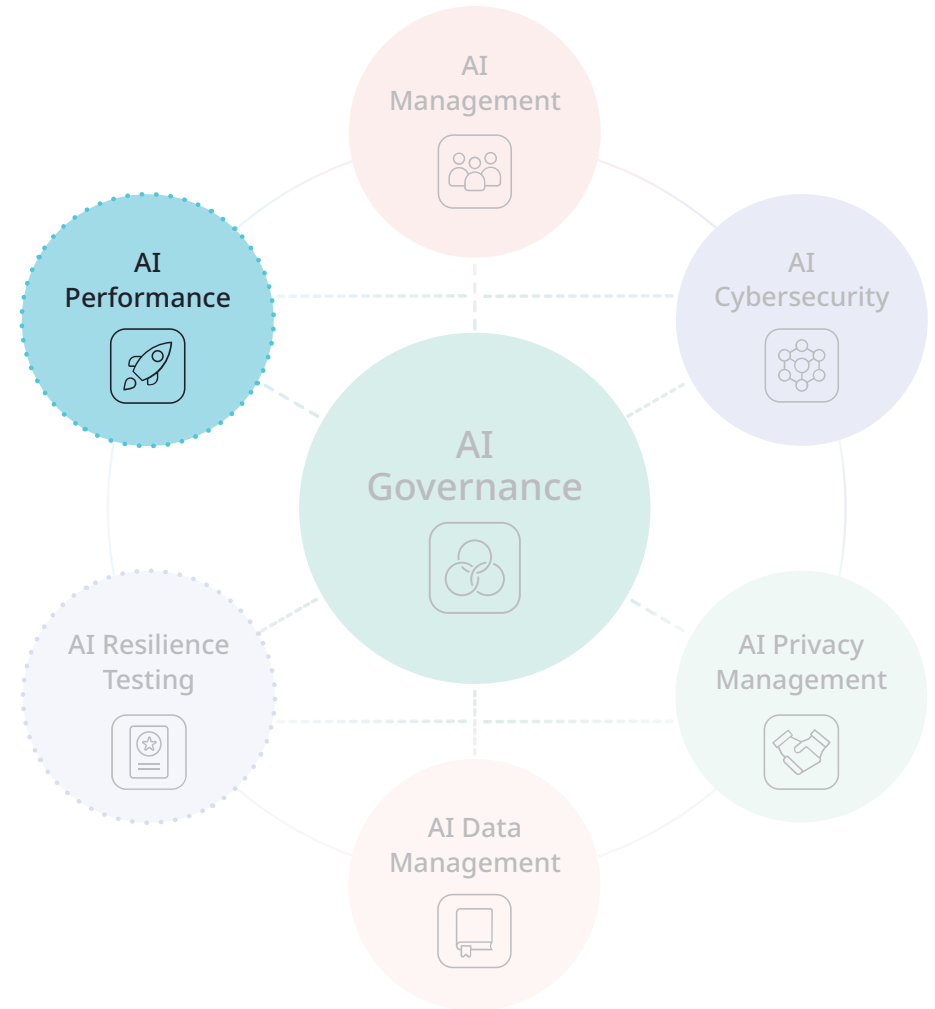
- 본 모듈은 자가진단을 포함하지 않습니다.
- 검증을 위해 AI 성능 지표를 제출합니다.

3. 테스트

- 8개의 국제 표준 기반 평가 기준을 적용한 성능 검증
- 회귀 분석
- 이진·다중·멀티라벨 분류
- 객체 탐지
- 시맨틱 분할
- 생체 인식 식별 및 검증

4. 결과

- AI 성능 테스트 보고서 제공
- 확인서 발급
- BSI 트러스트 마크



신뢰할 수 있는 AI 표준 전문가

BSI는 AI 도입에 대한 신뢰 구축을 지원하는 독보적인 역량을 보유하고 있습니다.



표준 개발 기관

AI, 정보보안, 개인정보보호 등의 국제 표준 개발에 참여해 왔으며, 125년 이상 표준 분야를 선도해 왔습니다.



전문 교육

BSI Training Academy를 통해 수천 명의 전문가가 역량을 향상시켰으며, AI 및 디지털 트러스트 분야에서 20개 이상의 교육 과정을 제공합니다.



독립적 인증 역량

BSI는 AI 경영시스템 분야에서 영국 인정기구(UKAS)의 인증을 획득한 최초의 인증기관입니다.



글로벌 역량과 현지 지원

전 세계 AI 전문 강사 및 심사원 네트워크를 통해 어디서나 동일한 수준의 서비스를 제공합니다.



BSI 트러스트 마크

BSI Mark of Trust는 조직의 AI 역량이 BSI에 의해 독립적으로 검증되었음을 증명하는 글로벌 신뢰의 상징입니다.



Your partner
in progress

bsigroup.com