DB보안을 위한 핵심 점검 포인트

# Advanced DQC-S

11th 2013 Database Grand Conference


## 1. 들어가는 글



## 2. Advanced DQC-S 소개

KODB 한국데이터베이스진흥원 KOREA DATABASE AGENCY

## 01. DQC-S 개요

DQC S 데이터보안인증

**DQC-S(데이터 보안 인증, Database Quality Certification-Security)**

**2012.04.30 "데이터베이스품질인증제도"**로부터 출발

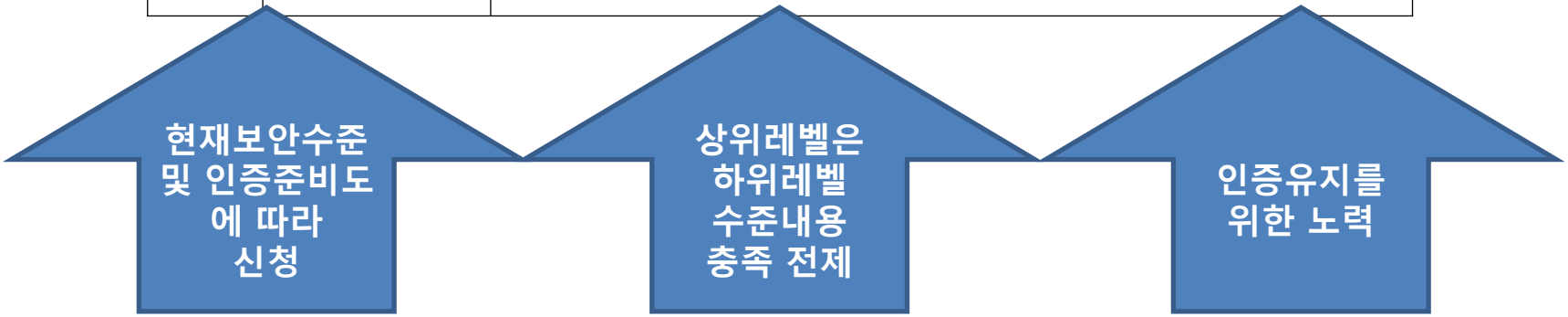
**2010.11.22 한국데이터베이스진흥원, "데이터베이스품질인증기관지정"**으로 인증심사 시행

**DQC-S 인증모델은**

DB보안의 핵심 기술로 **"접근제어, 암호화, 작업결재, 취약점분석"** 등을 선정, 공공·민간에서 구축·활용 중인 **데이터베이스를 대상으로 위의 핵심 기술 전반을 심사, 인증** 하는 것

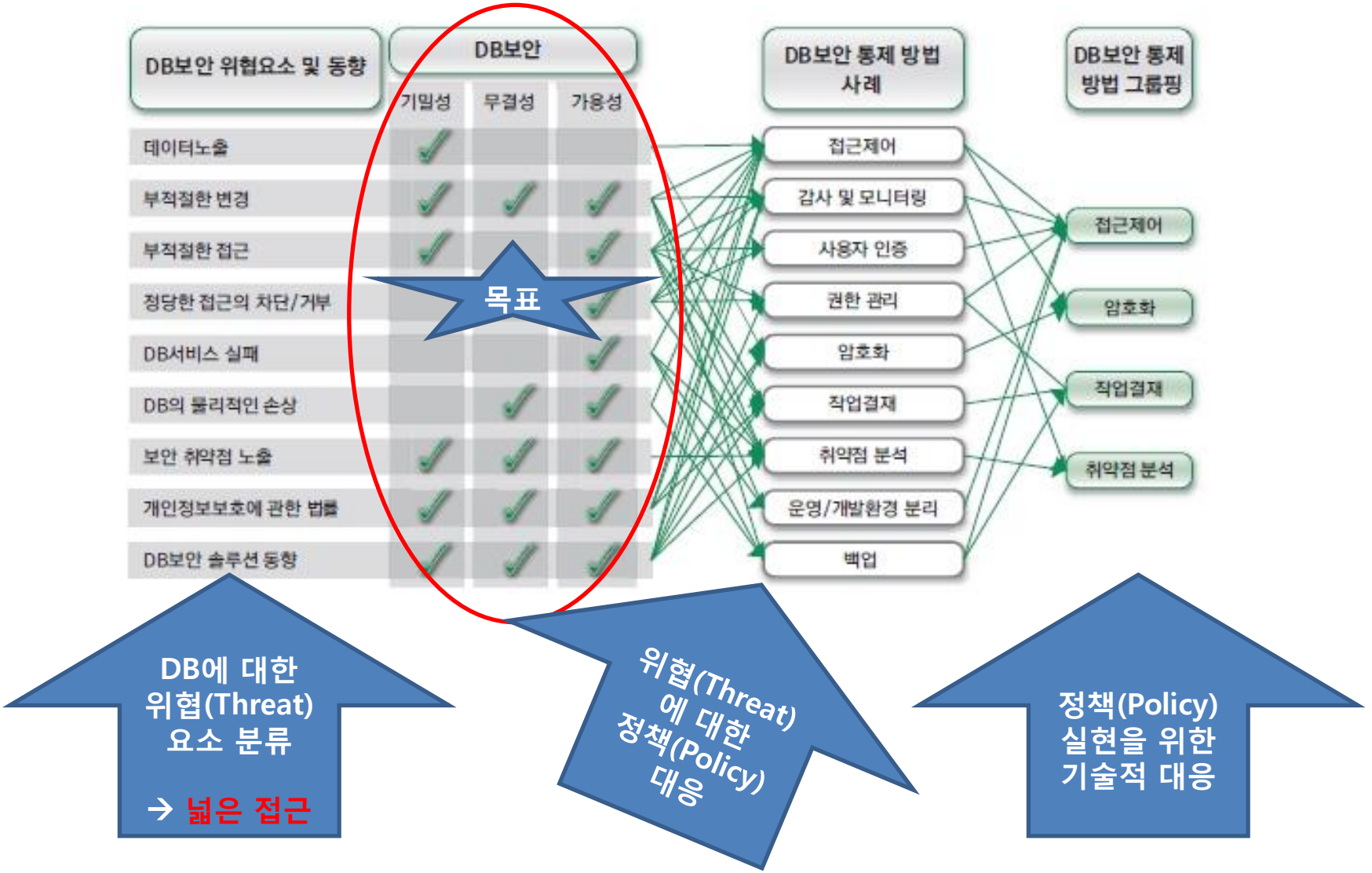
## 02. DQC-S 인증 레벨

| 구분 | | 수준 내용 |
|---|---|---|
| 4레벨 | **취약점분석** | DB의 취약점을 다각적으로 분석하여 보완하는 단계 |
| 3레벨 | **작업결재** | DB작업의 정당성을 확보하기 위해 결재를 수행하는 단계 |
| 2레벨 | **암호화** | 중요 정보를 암호화하여 정보 유출에 대비하는 단계 |
| 1레벨 | **접근제어** | DB로의 접근 행위를 제어, 관리, 기록하는 단계 |



KODB 한국데이터베이스진흥원 KOREA DATABASE AGENCY

## 03. DQC-S Framework – 보안기술 요소



KODB 한국데이터베이스진흥원 KOREA DATABASE AGENCY

## 03. DQC-S Framework – DB보안 프레임워크 / DB보안 관리 프레임워크

| | 접근제어 | 암호화 | 작업결재 | 취약점 분석 |
|---|---|---|---|---|
| 기획 | DB 보안 정책수립 | | | |
| 설계 | 접근제어 규칙 정의 | 복호화 권한 통제<br>암호화키 및 알고리즘 정의 | 작업결재 규칙 정의 | 취약점 분석 계획 |
| 구축 | 우회 접근 방지 | 원본 데이터 삭제<br>제약 사항 유지<br>암호화 키 관리 | 우회 결재 방지 | 모의 해킹 |
| | 환경 보완 | | | 내부보안 감사 |
| | 보안 적용 시험 | | | |
| 운영 | 보안규칙관리 | | | 취약점 수집 |
| | 사용자 로그 관리 | | | 취약점 제거 |
| | 모니터링 | | | 취약점 개선<br>분석 비교 |
| | 운영 리뷰 | | | |

DB보안을 위한
기획→설계
구축→운영→관리
선순환을 이루는 구조

조금은 매끄럽지
않은 Process

KODB 한국데이터베이스진흥원 KOREA DATABASE AGENCY

## 04. DQC-S Check List

| 심사항목 | 세부항목 | 점검내용 |
|---|---|---|
| 접근제어 | 접근제어 정책수립 | •접근제어 정책 수립 여부 |
| | 접근제어설계 | •접근제어 규칙 정의 여부 |
| | 접근제어구축 | •접근제어 구축 수준 |
| | 접근제어 운영 | •접근제어 운영 수준 |
| 암호화 | 암호화 정책수립 | •암호화 정책 수립 여부 |
| | 암호화 설계 | •암호화 설계 수준 |
| | 암호화 구축 | •암호화 구축 수준 |
| | 암호화 운영 | •암호화 운영 수준 |
| 작업결재 | 작업결재 정책수립 | •작업결재 정책 수립 여부 |
| | 작업결재 설계 | •작업결재 규칙 정의 여부 |
| | 작업결재 구축 | •작업결재 구축 수준 |
| | 작업결재 운영 | •작업결재 운영 수준 |
| 취약점분석 | 취약점분석 정책 수립 | •취약점분석 정책 수립 여부 |
| | 취약점분석 설계 | •취약점분석 규칙 정의 여부 |
| | 취약점분석 구축 | •취약점분석 구축 수준 |
| | 취약점분석 운영 | •취약점분석 운영 수준 |

## 05. 데이터베이스 보안 가이드라인


기술 성숙도를 따를 수 있어야
내재화를 위한 효용성을 높여야
국제 표준화를 선도해야


## 2. Advanced DQC-S 소개

KODB 한국데이터베이스진흥원 KOREA DATABASE AGENCY

## 01. Database Security 참조모델

| | Role Type | | | | | DQC-S |
|---|---|---|---|---|---|---|
| | Privileged Users | End Users | Developers, System Analysts and System Administrators | IT Operations | Malicious Users | |
| Access to, deletion of, or changes to data: | M | NA | NA | NA | NA | DAP |
| Access using inappropriate or nonapproved channels: | M | NA | NA | NA | NA | DAP, VA |
| Schema modifications: | M | NA | NA | NA | NA | DAP |
| Unauthorized addition of user accounts or modification of existing accounts: | M | NA | NA | NA | NA | DAP, VA |
| Access to excessive amounts of data or data not needed for legitimate work: | NA | M | NA | NA | NA | DAP, WF |
| Access to data outside standard working hours: | NA | M | NA | NA | NA | DAP, WF |
| Access to Sensitive Data | NA | M | NA | NA | NA | ENC |
| Access to live production systems: | NA | NA | M | NA | NA | DAP, MSK |
| Unapproved changes to databases or applications that access the database: | NA | NA | NA | M | NA | DAP |
| Out-of-cycle patching of production systems: | NA | NA | NA | M | NA | Operatoinal Management Policy |

M: Monitoring and Blocking
NA: Not Allowed
DAP: Database Audit and Protection
ENC: Encryption
WF: Workflow
VA: Vulnerability Assessment
MSK: Data Masking

Privileged Users: DBA
End Users: Groupware, Applications
Developers, System Analysts and System Administrators: Including Outsource Engineers
IT Operations: Including Outsource Engineers

**Discovery and Define**
1. Discover where sensitive data resides
2. Classify and define data types
3. Define security policies and metrics

**Secure and Protect**

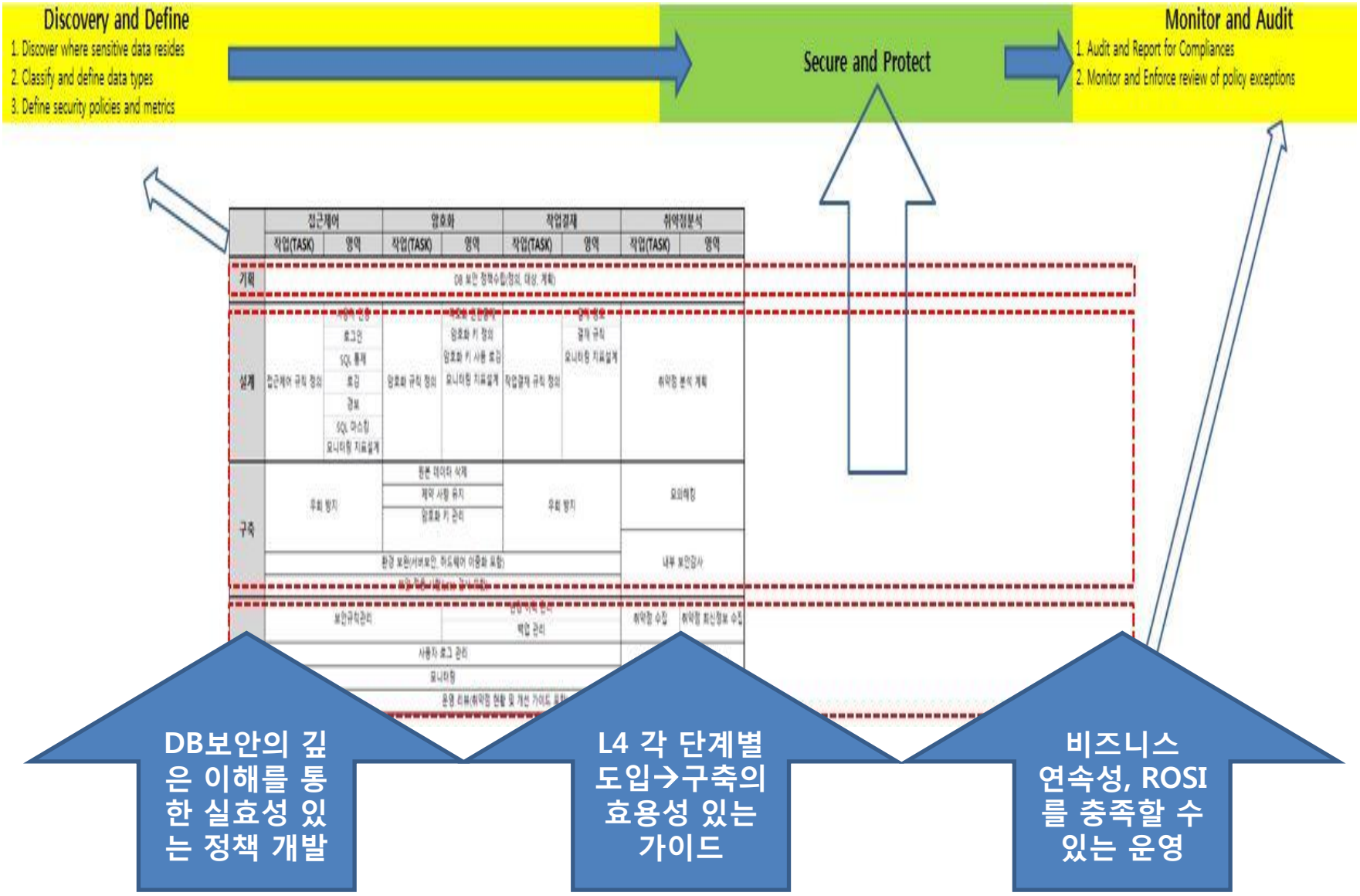
**Monitor and Audit**
1. Audit and Report for Compliances
2. Monitor and Enforce review of policy exceptions

Data Service 전체를 관통 할 수 있는 **규정/정책 기획**

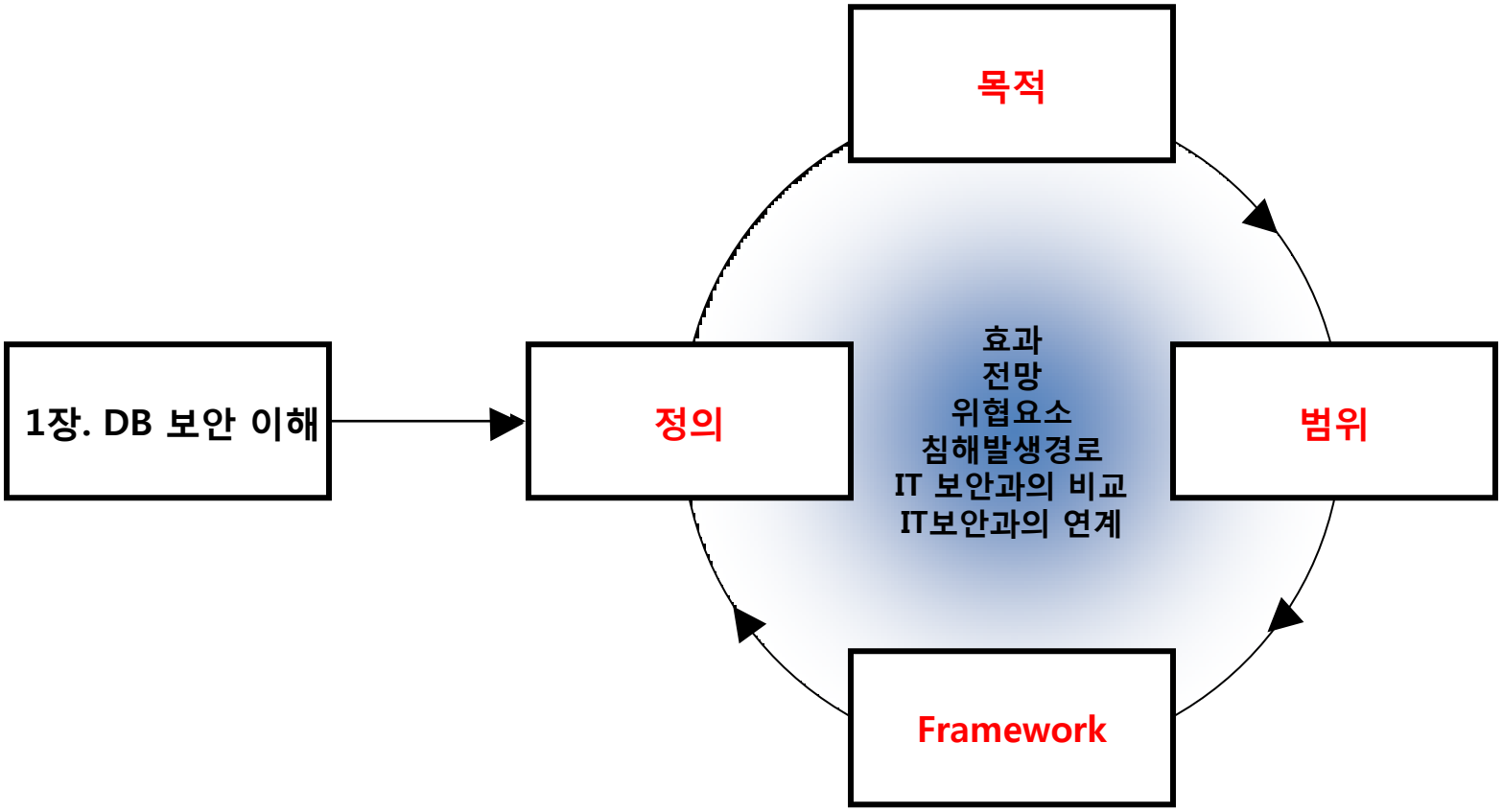
**규정/정책** 심화적용 할 수 있는 **시스템 구현**

Reactive Pro-active Planning 가능한 **S-거버넌스**

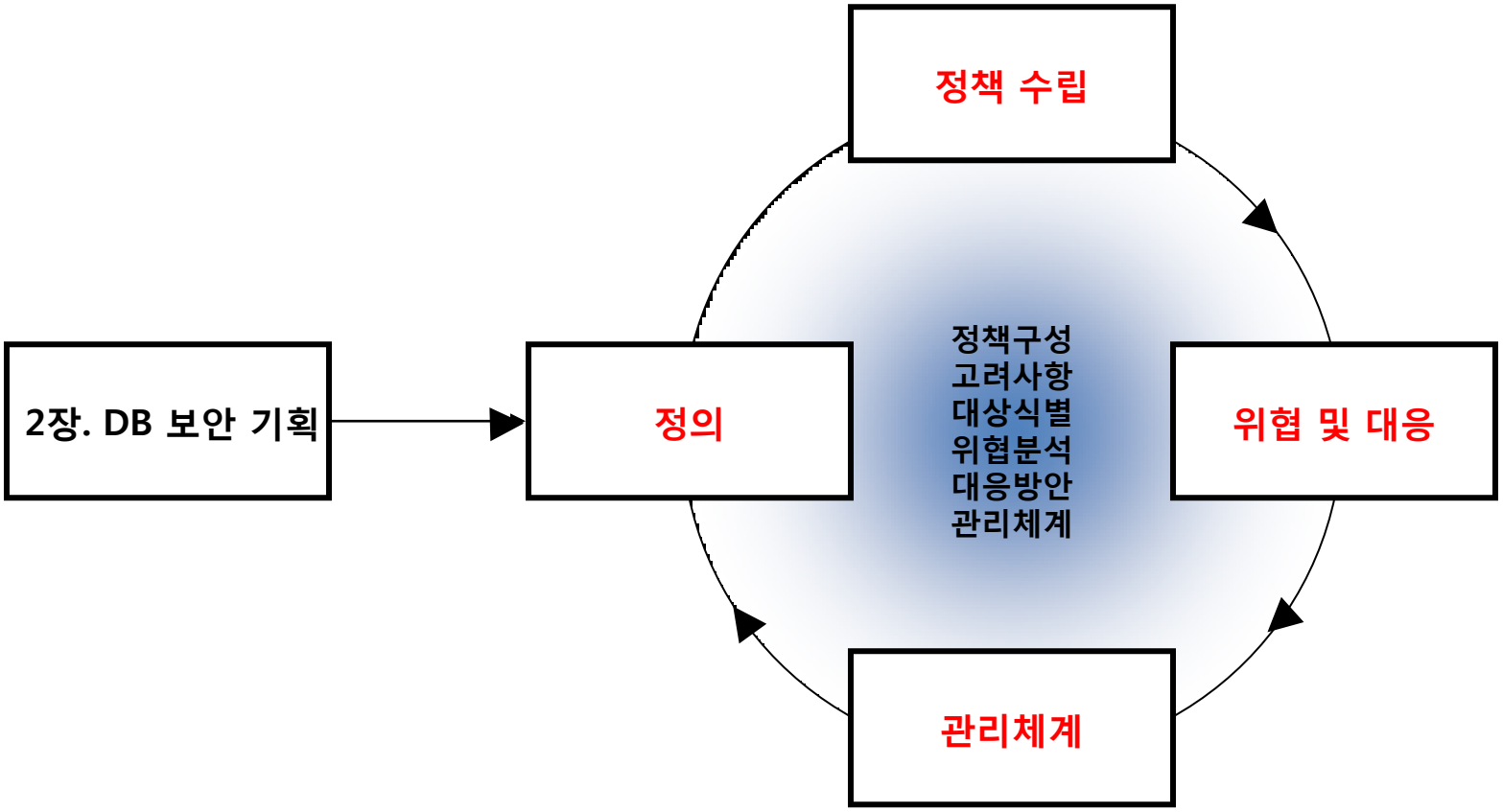
## 02. Old vs. Advanced



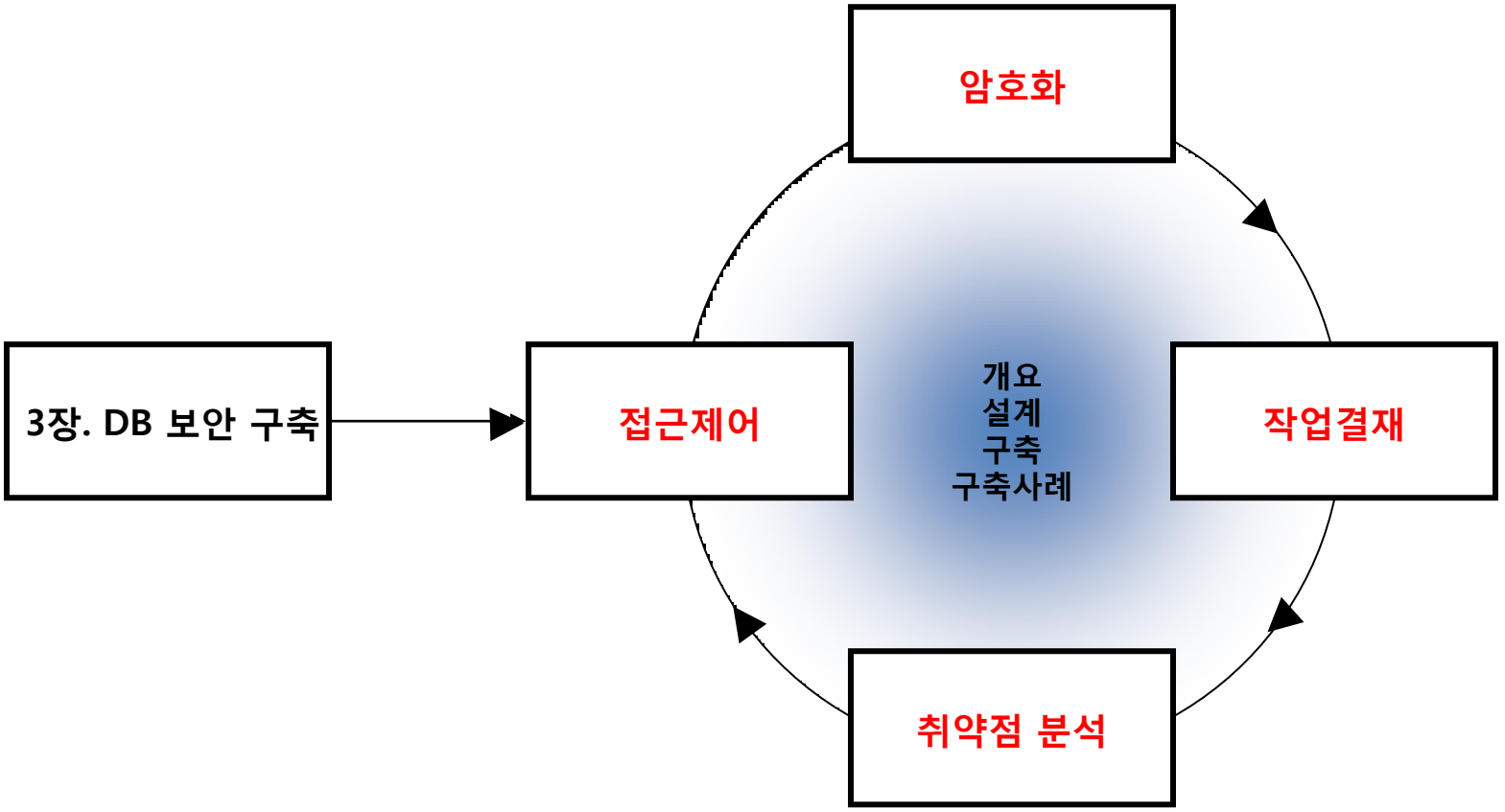
## 03. Advanced DQC-S 가이드라인의 구성(1)



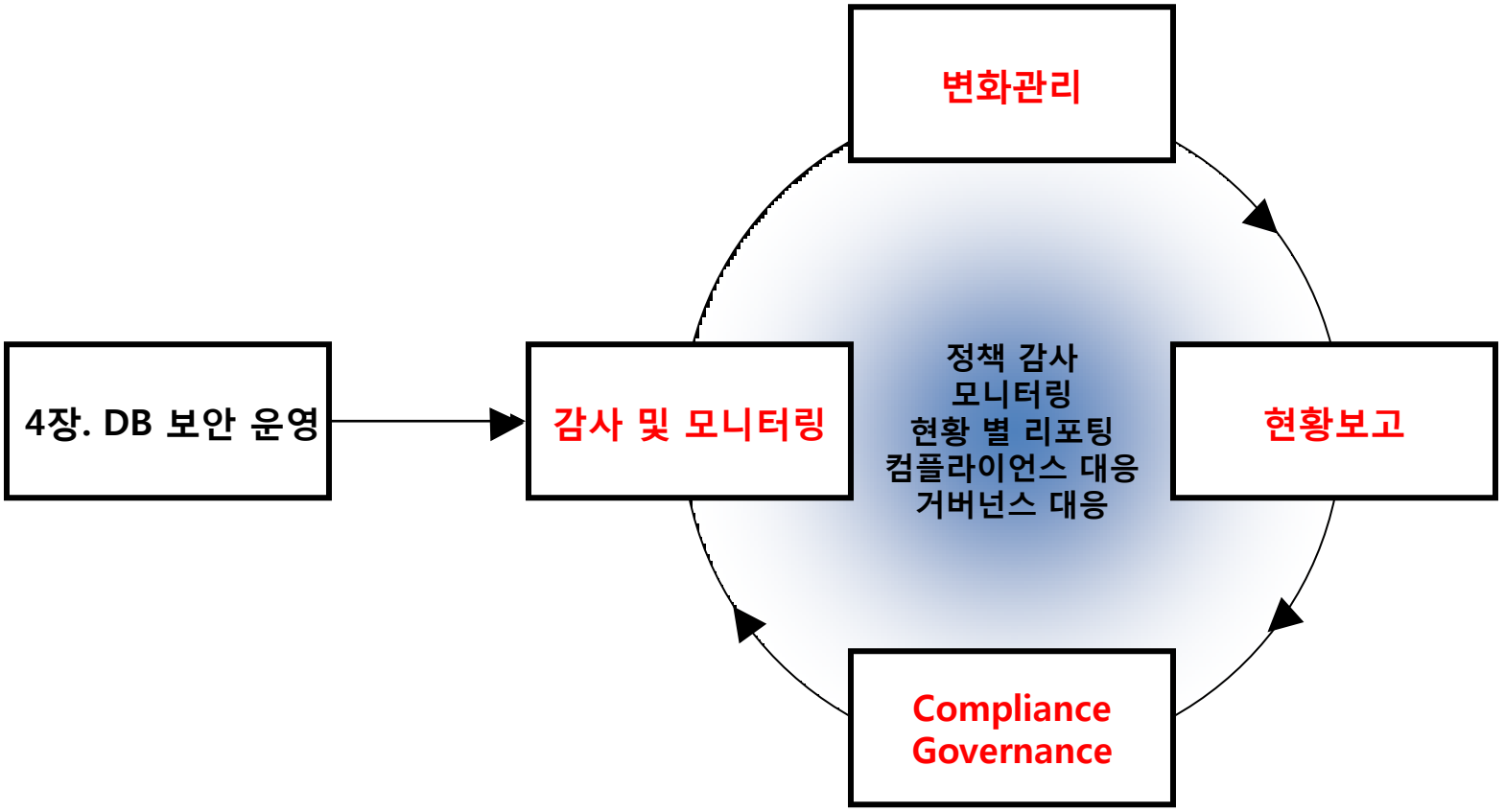
## 03. Advanced DQC-S 가이드라인의 구성(2)



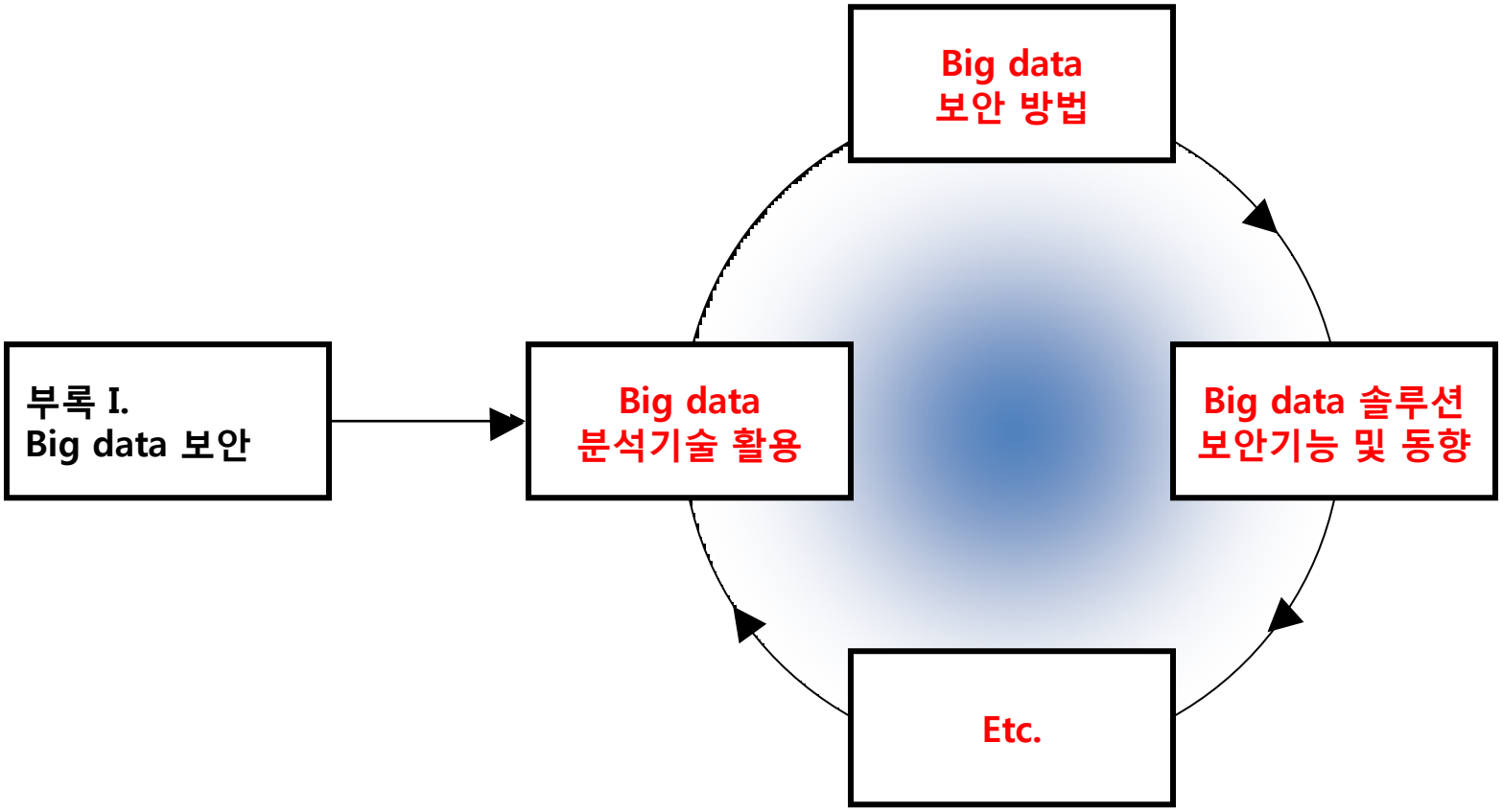
## 03. Advanced DQC-S 가이드라인의 구성(3)



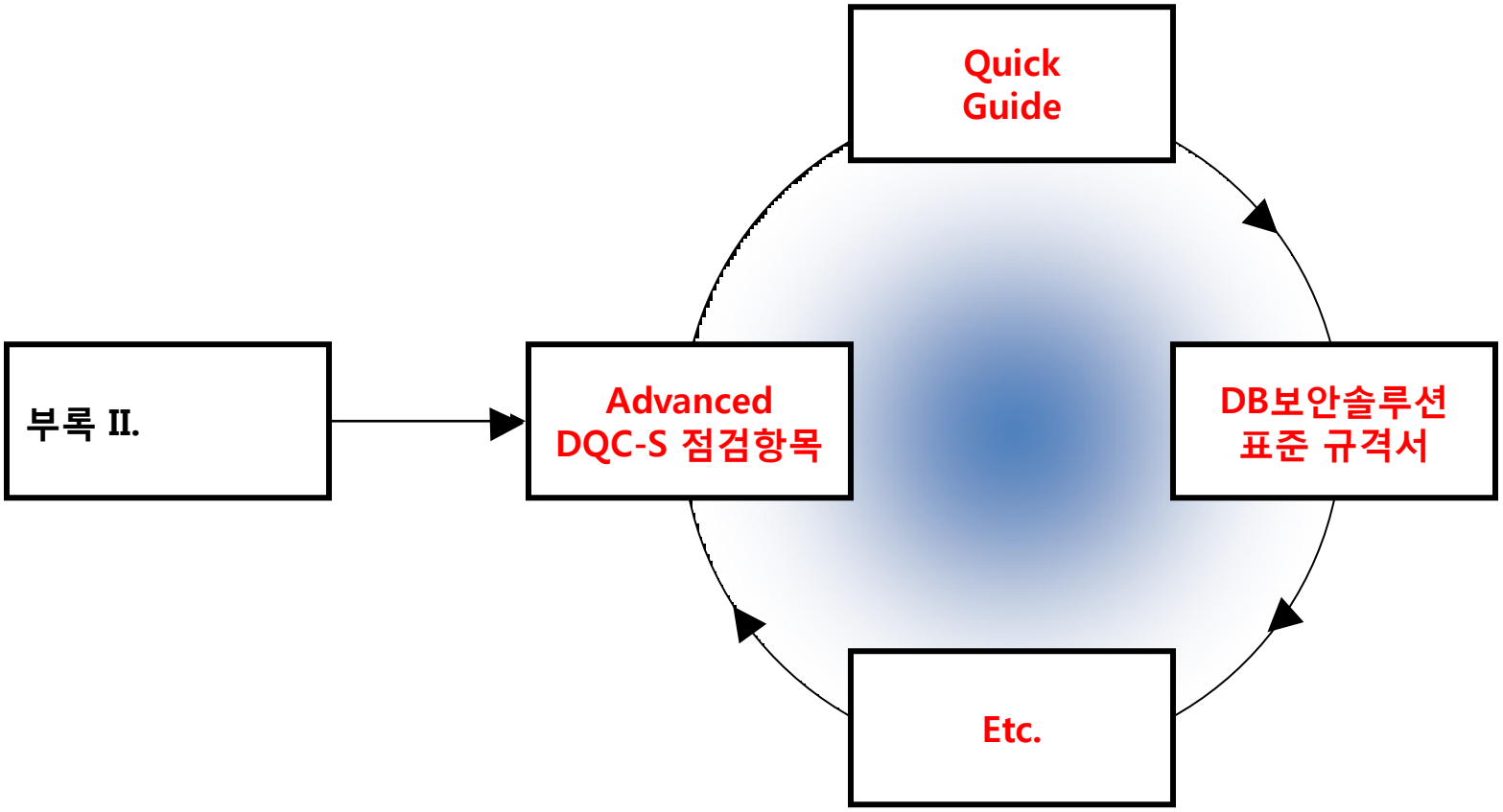
## 03. Advanced DQC-S 가이드라인의 구성(4)



## 03. Advanced DQC-S 가이드라인의 구성(5)



## 03. Advanced DQC-S 가이드라인의 구성(6)



# Advanced DQC-S


**Coming Soon!!!**

# Thank you

발표자 : ㈜유젠아이 조응진