Deloitte.

GRC-Sustaining compliance and risk (Governance, Risk and Compliance)

2008. 9. 14

이종익 이사

딜로이트기업리스크자문본부
(jongicklee@deloitte.com/010-5410-2310)

ORACLE

목차

- 글로벌 경영환경의 변화
- 위험 관리의 필요성
- GRC 의 필요성
- GRC 의 요소
- GRC 시스템의 필요성
- GRC 시스템의 기능별 영역
- GRC 의 효과
- GRC 성숙도 모델
- 결론

Global 경영환경의 변화 – 평평한 세계 (통합, 경쟁, 투명, 복잡, 위험)

Deloitte.

글로벌 통합

인력, 기술, 자원, 자본

FTA

글로벌 무한경쟁
시장 진출/입에 대한
정부개입의 축소
(규제완화)

SOX 등의 재무 보고 규제
환경규제

무역규제

(규제강화)

객관적인 투명성

합리적 거버넌스 요구

ORACLE

Global 경영환경의 변화 – 다양한 형태의 경영 위험

Deloitte.

87% Risks are not Financial

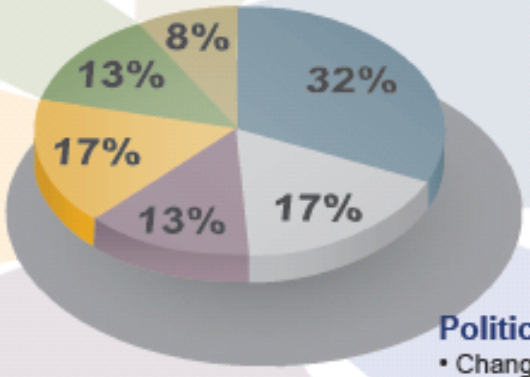
Operational
- Hurricane Katrina
- Data center outage
- Delivery risk
- Blast furnace cold run
- ERP application crash
- Plant disaster causing production stoppage

Legal & Compliance
- Fraud
- Product liability claims
- Missed time line for legal changes
- Embezzlement of parts
- Safety of goods or products

Material risk events encountered in the past three years (for enterprises over US$5 billion in revenue).

Strategic
- Industry consolidation and globalization
- Error-filled release of software upgrade
- Change in core product demand
- Cancellation of major customer contracts
- Performance standards and service quality

Environmental / Health
- West Nile Virus
- Safety crisis
- Compliance with environmental standards
- Food sanitary management problem
- Climate change
- Environment pollution



Political/Geopolitical
- Change of government – and minority governments
- Grants and budget changes
- Constant change of ministers
- Federal Accountability Act
- Terrorism

Financial
- Currency exchange rates
- Interest issue and increasing reserves
- Accuracy of realistic balance sheet reporting
- Ability to manage cash
- Non-transparent markets
- Economic recession
- Energy and commodity costs

Source: IBM Global Business Services, The Global CFO Study 2008.

ORACLE

Global 경영환경의 변화 – 규제의 성격에 따른 위험 증대

Deloitte.

상기와 같은 환경에서 규제는 정부에 의한 국가별 획일적 규제로부터 **시장 감시 및 국제 기준을 강조**하는 새로운 규제로 성격이 바뀌게 됨

- 기업의 재무 보고 과정과 공시기준 강화: SOX와 내부 회계관리제도, 증권 관련 집단소송법
- 금융기관의 건전성 관련기준 강화: BASELII
- 회계기준의 통일과 강화: IFRS
- 품질 · 환경기준의 강화: ISO, REACH, RoHS, WEEE
- 기타 법적 규제의 강화: 공정경쟁, 소비자보호, IPR, 작업장안전

이러한 규제 환경에 따라 다양한 형태의 위험이 기업의 생존을 위협하고 있음

- Enron, Worldcomm 분식회계
- SK Global 분식회계
- IMF 외환위기
- 1파운드에 팔린 Barings Bank
- 주당 10불에 팔인 Bear Sterns 의 몰락
- 삼성특검
- 현대차비자금
- 태안 기름유출

Global 경영환경의 변화 – 현재의 규제

Deloitte.

Global Regulation

- THE Sarbanes-Oxley(SOX)
- BASEL II
- IFRS
- REACH(화학물질 관리규정)
- ROHS(특정유해물질 사용제한)
- WEEE(전기,전자장비폐기물처리지침)
- Eup(에너지사용제품관련지침)
- ELV(폐 자동차 처리지침)
- HIPAA(의료정보보호법)
- IT Governance (COBIT)
- 내부회계관리제도 (COSO)
- NIIPA(개인정보보호법)
- 자본시장통합법
- 증권관련 집단소송법
- 기후변화협약에 따른 규제
- ISO인증 (품질,환경 등)
- FTA에 따른 지적재산권 및 특허권

시행예정

- BASEL II (2008년~2009년)
- IFRS (2009년~2011년)
- 자본시장통합법 (2009년)
- 기후변화협약 규제 (미정)
- 지속가능경영-ISO26000인증 (미정)

현행

- SOX(NYSE상장기업)
- 내부회계관리제도
- 기업체 특성에 따른 REACH/ ROHS/ WEEE/ Eup/ ELV 등 (EU대상 수출업)
- IT Governance
- 집단 소송제
- 지적재산권법
- 전자금융거래법

✓ 회사의 책임자(CEO, CFO등 주요 경영층)들의 회사활동에 대한 책임의무가 강화됨

✓ 전사차원의 규제 적용

기업이 준수하고 따라야 할 규제 및 규범은 지속적으로 증대 될 것으로 예상

위험 관리의 필요성 - 실패 사례

Deloitte.

Fortune 1000대 기업 중 50%는 위험관리에 실패하여 주식가치가 20%이상 하락. 그 중 22%는 회복 못함

국내 사례

- 환경규제 준수 실패
  - 대미 수출상품에 오존 파괴 물질 사용함으로써 과징금 20만$ 부과
- 운영측면에서 발생한 위험
  - 공장 라인 중단 사태로 인해 500 억 원 이상 손실
- 국제 무역 규제 실패
  - EU 환경 물질 신고서 누락으로 물품 통관 거부로 반송

해외 사례

- 내부통제 실패
  - 홍콩 법인 금속 선물 손실만회를 위한 내부 은폐 및 거래로 인해 950억 손실
- 외환관리 실패
  - 부실 자산으로 인해 10 년 간 매 해 1000 억 원대의 외환 손실
- 규제 준수 실패
  - 준수 실패 하루 후 기업 가치 50%하락
- 규제 준수 실패
  - FDA 준수 실패로 영국 백신 공장 파산

재무적인 손실뿐 아니라 브랜드이미지에도 막대한 타격 발생

위험 관리의 필요성 - 실패로 인한 영향

Deloitte.

통제 취약점이 발견된 경우 사업 수행 장애

심각한 수준의 규제 미 준수 이슈 발생 시 하루 만에 50%의 기업 가치 손실이 발생하는 경우도 있음 (예 Adecco.)

공표된 규제 미 준수 이슈가 존재하는 기업의 투자 비용은 그렇지 않은 기업에 비해 현저하게 높음.

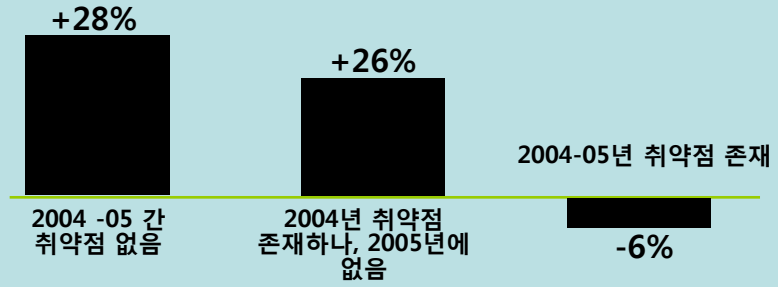
Price of control deficiency for $1 billion company

$10 million

자기자본비용 증대

Source: University of Wisconsin, 2006

기업의 규제 준수 실적에 따른 주식 가치 영향도 분석



Source: Lord & Benoit, 2006

화이저 제약은 기업 청렴도 협정을 준수하기 위해 4억3천만 달러 이상을 지출함.

FDA의 안전 기준을 준수하기 위해 영국의 백신 공장의 생산이 중단됨

유럽의 물류보안 인증제도(AEO)를 준수하지 못하는 기업들은 운송 상의 지연을 겪고 있음.

ORACLE

위험 관리의 필요성 – 기업의 생존 (지속 경영, 안정성, 신뢰성)

Deloitte.

현대의 기업 환경에서는 위험에 노출되어 이에 대한 대비를 하지 못하는 경우 **즉시적으로 경영이 중단**되는 등 속도와 영향의 폭이 매우 **크므로 불확실성과 위험관리는 지속가능 경영의 필요조건**으로 자리 매김됨

이상의 환경변화에 대응하여 기업, 특히 상장기업에 대한 투자자, 금융기관, 정부 등 **이해당사자의 요구가 강화**되었음. 이에 따라 기업은 다음과 같은 위험 관리 능력을 갖추도록 요구됨

-경제적 의사결정에 필요한 (Adequate) 경영정보(계량+비계량)

-신뢰성(Trustfully)있게, 적시에(Timely), 충분하게(Fully), 공시(Disclose) 할 것

-경영정보를 생산하는 기업 내부 시스템(제도와 절차)이 제대로 가동 되도록 정보의 품질관리 시스템(Quality control and assurance system)을 갖출 것

-경영활동이 적법(Legitimately)하고 윤리적(Ethically)으로 수행 될 수 있는 체제를 갖출 것

-기업이 직면하는 외부의 법적 의무사항(Legal mandate)이 준수될 수 있는 체제를 갖출 것

-이상의 위험관리를 통합적으로 관리 할 수 있는 지배구조(Governance) 를 갖출 것

위험 관리의 필요성 – 개별 대응의 한계

Deloitte.

과거의 위험 관리 요구 사항

- 규제 미 준수로 인한 벌칙 방지
- 이벤트 발생 후 신속한 대응
- 예상하지 못한 실적악화 방지
- 자본비용의 증가 방지
- 경영 비효율 방지
- 개별 대응 위주로 준수 비용의 증가

현재의 위험 관리 요구사항

- 글로벌 규제환경
- 다국적 경영을 포함한 복잡한 경영 모델
- 경쟁 가속화
- 이해관계자의 힘 증대로 높은 수준의 경영정보에 대한 신뢰성 및 투명성 요구
- 이벤트 발생 전 체계적 대응
- 적시에 가시적 통합 정보의 제공

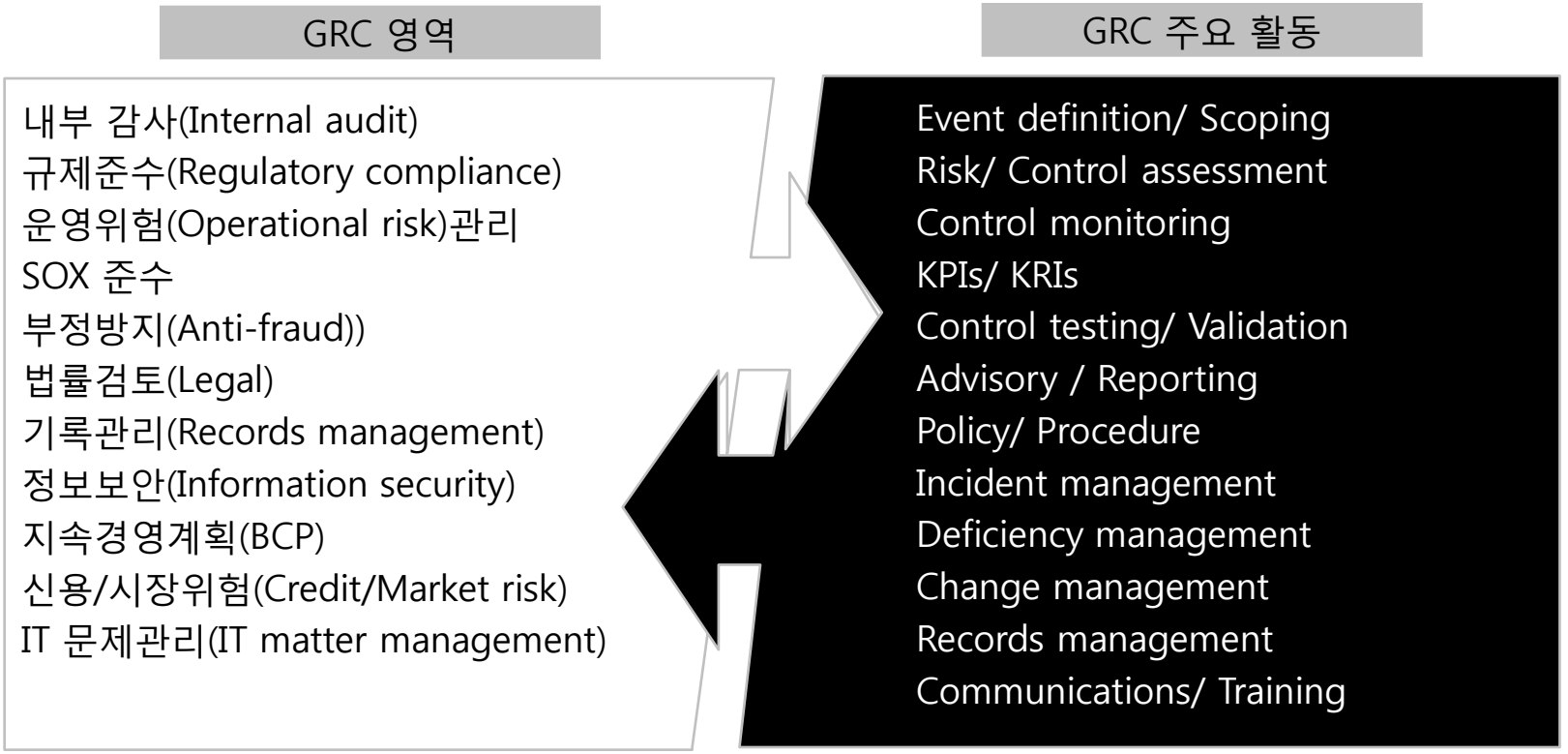
과거에는 위험관리와 규제준수를 각부서가 개별적으로 담당함

- IT : 정보보안, BCP, Privacy
- Compliance : 소비자보호, AML (Anti-money laundering)
- Risk Management: 부정방지, 신용위험, 운영위험, 시장위험, Basel
- Finance : 신용위험, Basel, 시장위험, SOX
- Legal : 소비자보호, AML, 부정방지, FSG
- Internal Audit : 전반적인 내부감사 역할

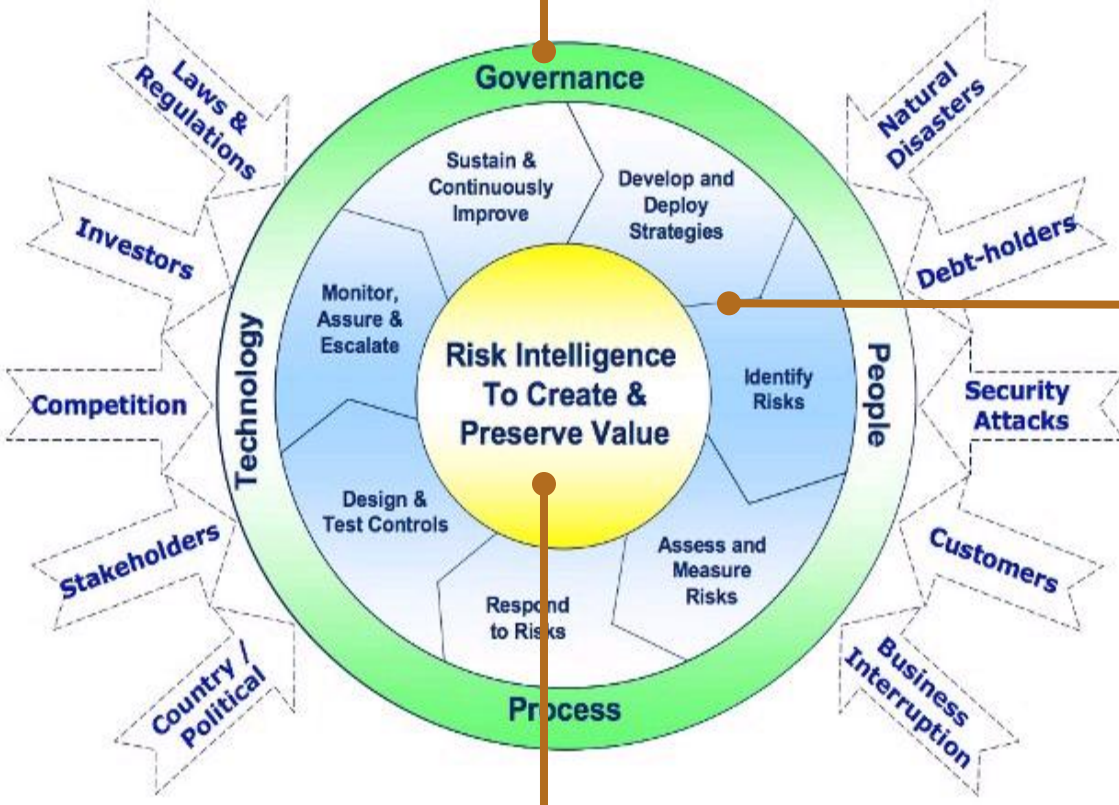
그러나 이제 추세는 Task-oriented compliance program으로부터 Process-oriented compliance program (지속적인 테스트와 확인)으로 바뀌고 있음 -> **GRC의 필요성 대두**

GRC 의 필요성 - 정의

GRC (governance, risk and compliance)는 기업이 **기업목표를 달성해 나가는 과정에서 직면하고 있는 장애물과 불확실성을 파악하고 이를 관리, 보증하는 프로그램과 조직화된 업무 절차**



GRC 의 필요성 - 정의



거버넌스 (Governance)
GRC 에 관련된 모니터링에 기반한 의사결정과 통제 체계
People: GRC 를 위해 필요한 인력 및 조직
Process: GRC 를 위해 전사적으로 적용되는 주요 활동
Technology: 대시 보드, 상시 모니터링 등 각종 도구 및 방법

위험관리 (Risk Management)
내, 외부 위험을 식별하고 관리하는 시스템

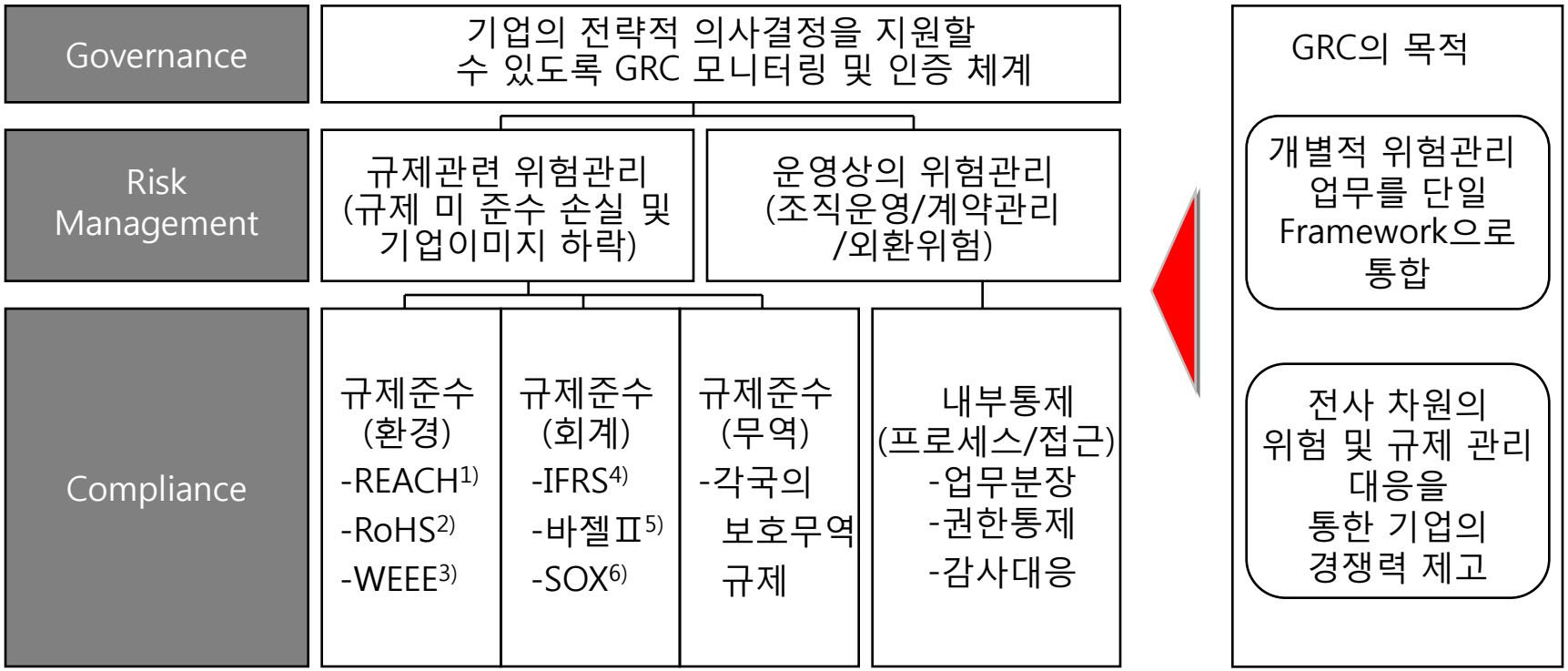
외부규제: 법적 책임, 준법감시 등
전략: 사업계획, 포트폴리오, 제품개발 등
재무: 시장, 신용, 유동성 등
프로세스: 프로세스 설계 통제, 운영 등
지배구조: 조직, 기업 운영 등
정보기술: IT, 경영정보보고, 데이터 관리 등

법규준수 (Compliance)
한정적인 기업의 자원을 최적화하여 환경, 무역, 회계 등 다양한 규제에 효과적으로 대응함

GRC 의 요소

Deloitte.

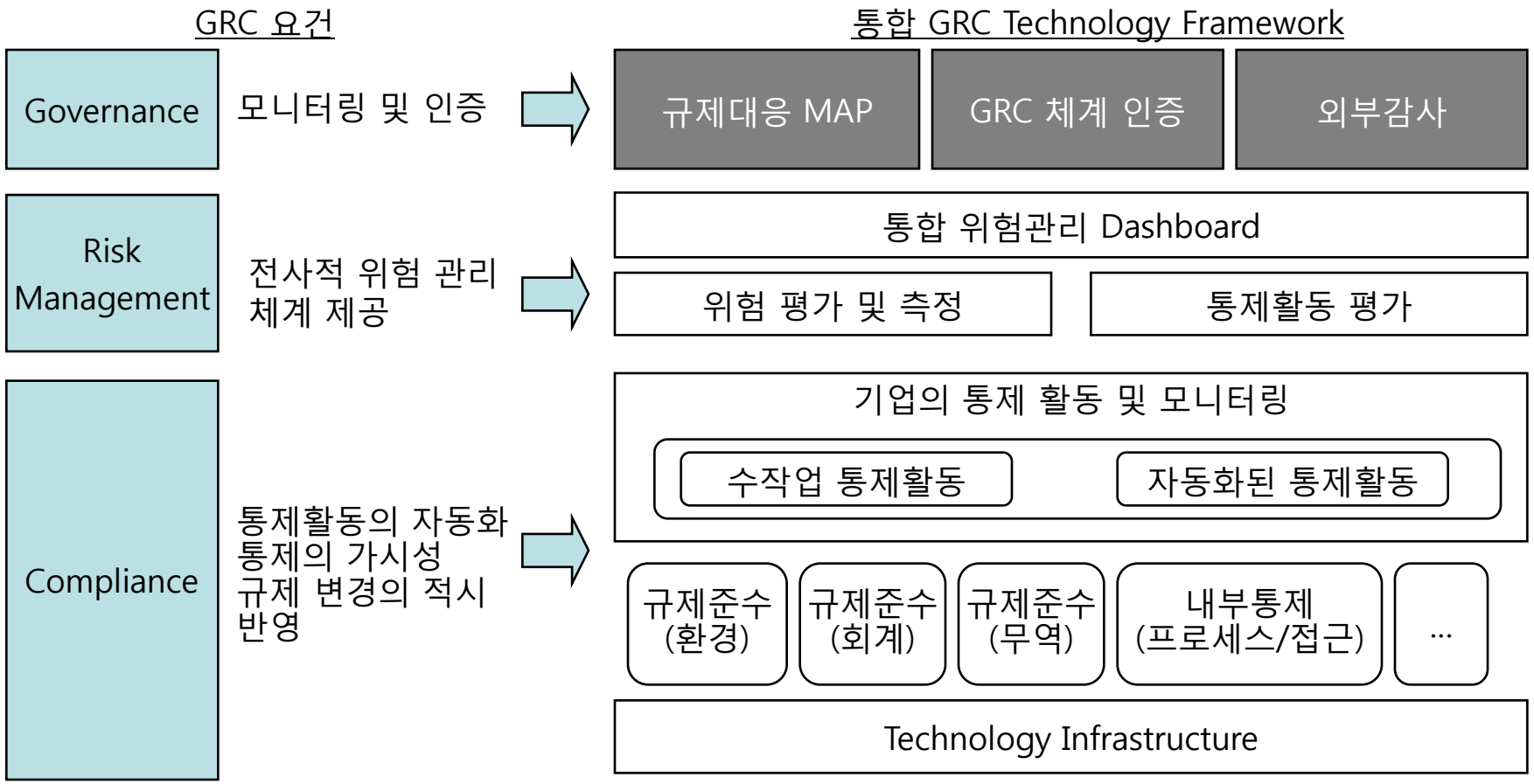
기업의 GRC 활동은 Governance, Risk Management, Compliance 각각의 영역이 유기적으로 연결되어 있으며, 기업의 경쟁력 제고를 위한 전략적인 목표와 연결됨



1) REACH (2007) :화학물질 안전성 입증 및 승인을 의무화하는 유럽연합의 신 화학물질 규제(Registration, Evaluation, Authorization & Restriction of Chemicals)
2) RoHS (2006) : 전기/전자제품 중 6개 물질(납, 6가크롬,카드뮴,수은, PBB, PBDE)에 대한 사용규제 (Restriction of Hazardous Substances)
3) WEEE (2005) : 폐 전기/전자제품 처리지침(Waste Electrical and Electronic Equipment)
4) IFRS (2011) : 2011년 1월 필수적으로 적용해야 하는 연결재무제표와 관련된 국제회계기준(International Financial Reporting Standards)
5) 바젤II (2007) : 신 자기자본에 대한 협약으로 금융업체가 보유하고 있는 자산에 대한 신용평가등급에 따라 자기 자본율을 차별 적용
6) SOX (2002) : 사내 견제와 균형을 통해서 경영의 투명성을 높이고, 경영진에 대한 책임 확대하는 규제(샤베인즈-옥슬리법)

GRC 의 요소 - Framework

GRC는 운영시스템의 정보를 활용하여 기업의 통제활동을 수행하고 위험/통제 수준을 평가하여 경영층의 가시성을 확보하는 체계로 구성



GRC 의 요소 – 세부 요건

Deloitte.

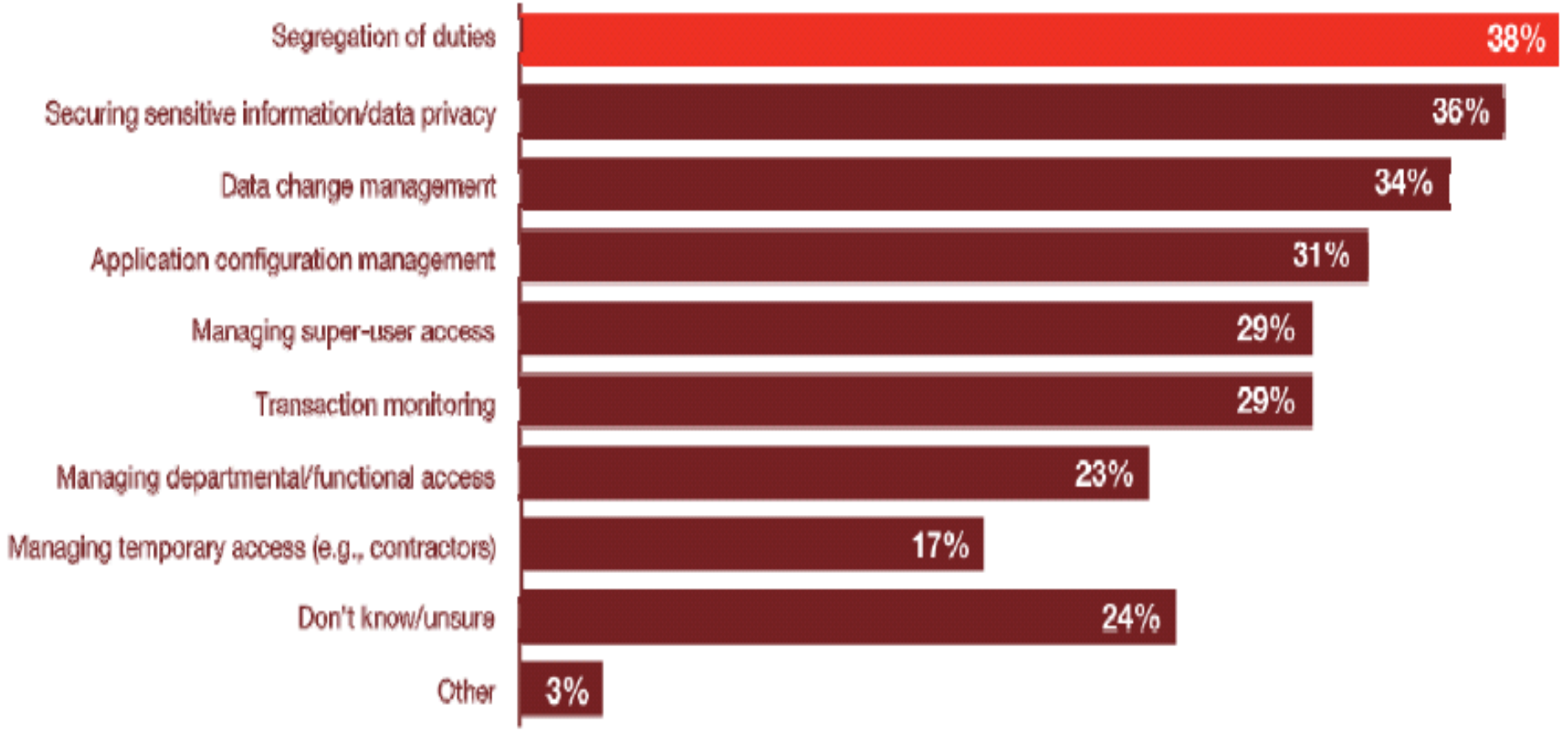
Governance	규제대응 MAP	• 규제 별 대응항목 및 관련시스템 체계 • 체계적 대응을 위한 업무정의서
	GRC체계인증	• CEO & CFO에 의한 내부 회계관리의 평가 및 인증
	외부감사	• 회계법인에 의한 외부감사 수행 결과 관리
Risk Management	통합위험관리 Dashboard	• 전사차원의 통합 위험관리 • 실시간 위험지표(KRI)확인
	위험평가 및 측정	• 위험 항목의 우선순위화 및 대응
	통제활동 평가	• 위험관리 통제활동 정의 • 통제활동의 추적 및 평가
Compliance	통제활동 모니터링	• 개별 업무별 이상상태 Summary • 수작업 업무처리 결과보고
	자동화된 모니터링	• 운영시스템에서 발견되는 이상 적발, 처리중지, 자동보고 • 역할에 따른 업무분장 검증
	수작업 모니터링	• 시스템에서 관리되지 못하는 업무/규정 준수 여부 확인 및 보고서 제출

GRC 시스템의 필요성 – 정보시스템 통제 취약점(한국)

Deloitte.

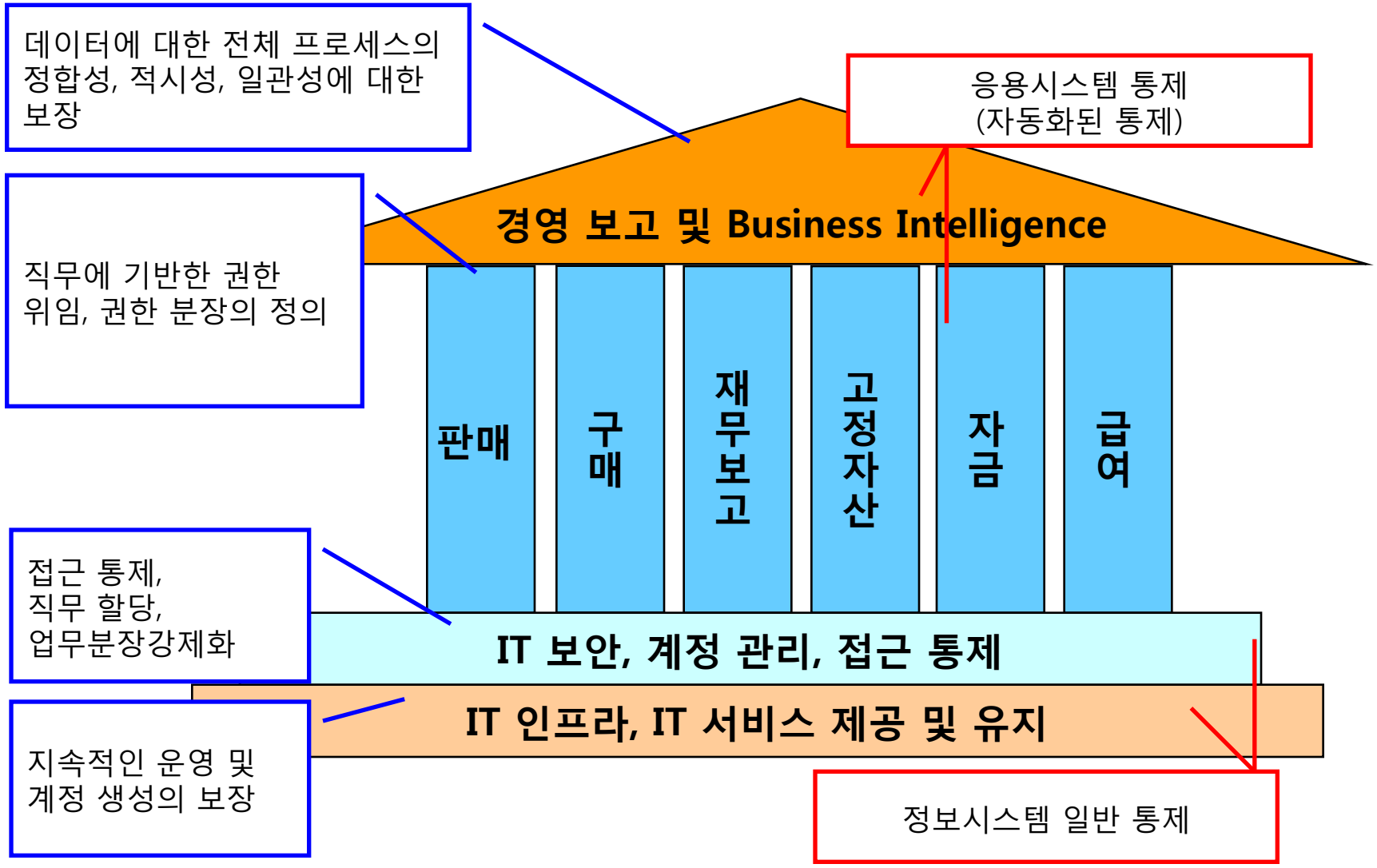
- 접근 통제 (Access Control) 에 대한 통제 취약점
  - Authentication (사용자 인증)의 미비
  - ID 의 공동 사용, 정직/퇴직자 ID의 사용
  - 접근 기록 유지 및 점검 기능 미비
- SOD (Segregation of Duties) 에 대한 통제 취약점
  - 자산 관리, 기록, 승인, 대사 등의 업무 분리 위반
  - 양립 불가 업무에 대한 통제 문제 (거래처 마스터 생성과 지급 업무, 계정 과목 마스터 관리와 전표 입력 업무, 주문 입력과 받을 어음 반제 업무 등)
- 업무 권한 (Authorization) 에 대한 통제 취약점
  - Super user 권한 및 과도한 일반 사용자에 대한 접근 권한 통제 미비
  - 업무 변경에 대한 권한 미 변경
  - 직무에 따른 권한 체계 미 설정
- 업무 프로세스 (Business Process) 에 대한 통제 취약점
  - 단위 프로세스 flow 상의 통제행위 누락 또는 무력화
  - 부정확한 프로세스에 대한 보고 및 점검 기능 미비
  - 통제 활동의 기록 및 승인의 미비
- 정보시스템 변경 관리에 대한 기록 미비 (시스템, 데이터, 프로그램 등)

GRC 시스템의 필요성 – 정보시스템 통제 취약점(미국)



Source: IT Role in GRC survey, Oracle, 2007

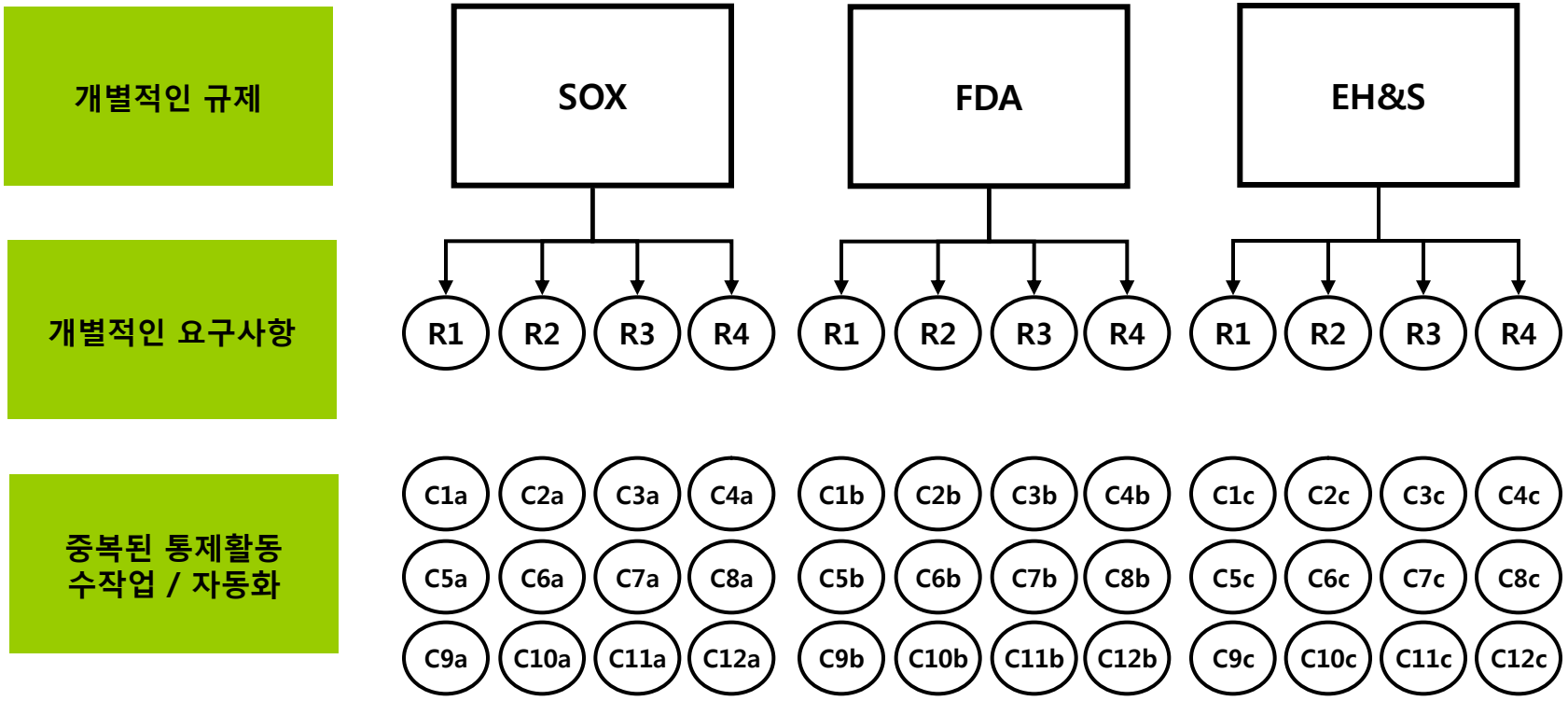
GRC 시스템의 필요성 – 정보시스템 통제의 영역



GRC 시스템의 필요성 – As-Is 시스템

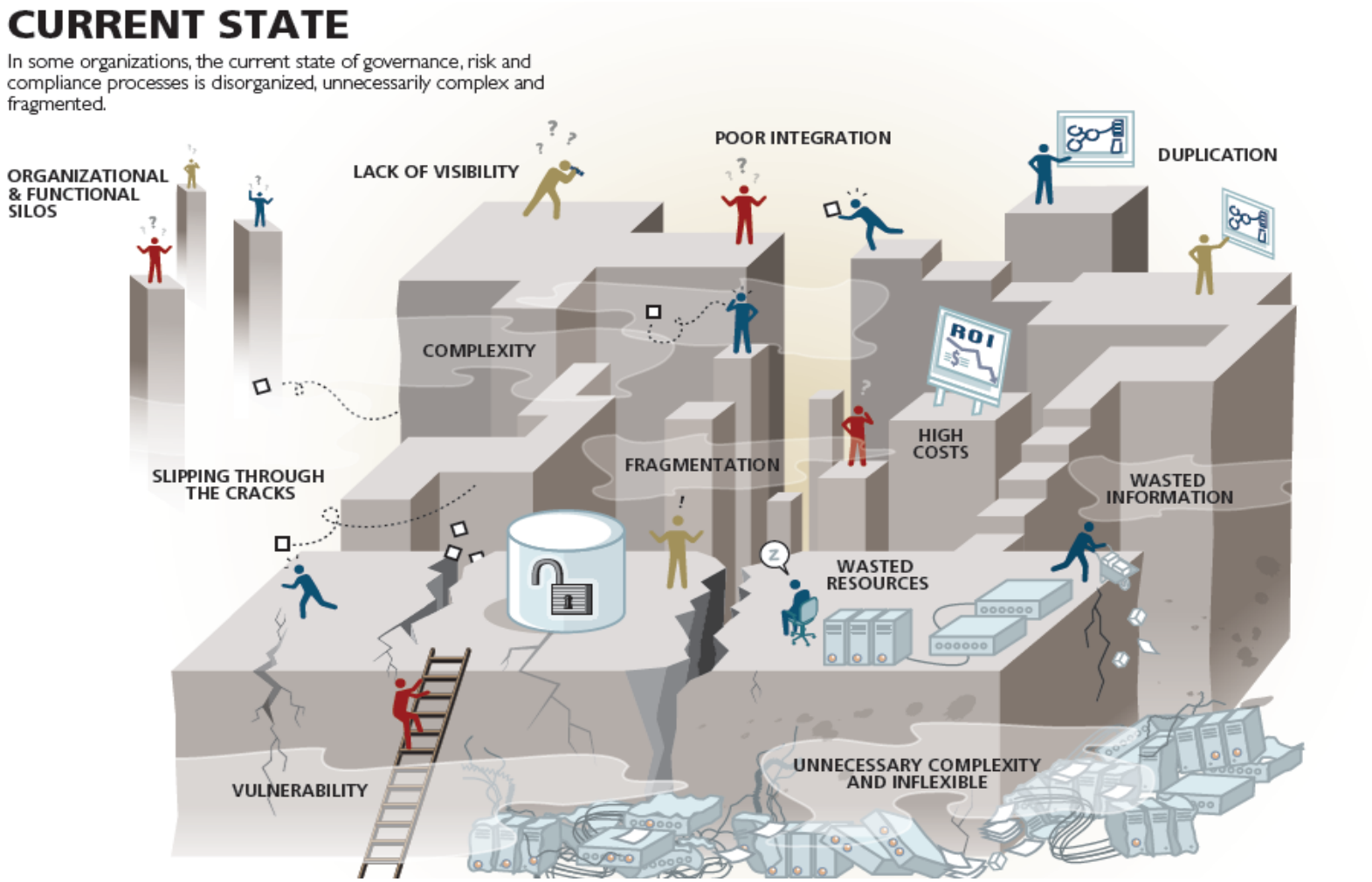
Deloitte.

각각의 규제는 많은 공통적인 요구사항을 포함하고 있으므로, 이에 대한 개별적인 접근은 통제활동에 대한 많은 반복적인 대응을 야기하여, 이에 따른 기업 자원의 낭비가 발생.



GRC 시스템의 필요성 - As-Is GRC: 복잡성, 고비용, 중복성

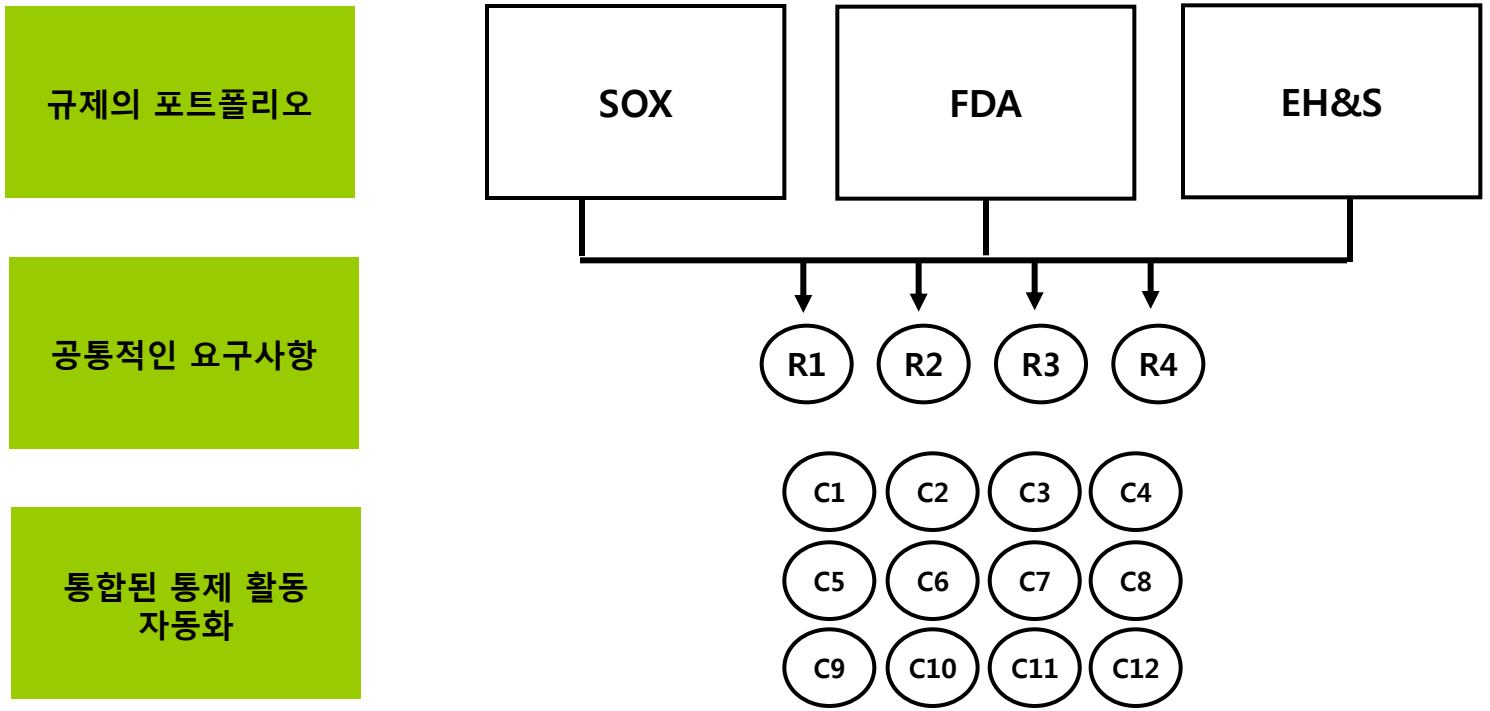
Deloitte.



GRC 시스템의 필요성 – 목표 시스템

Deloitte.

공통적인 요구사항과 공통적인 통제의 파악을 통하여 전사적으로 통합된 접근을 취할 경우, 복잡도와 중복된 통제, 노력 비용을 줄일 수 있음.



이와 더불어, 중복된 통제가 통합되면, 자동화된 통제로 얻을 수 있는 이득이 많아짐.

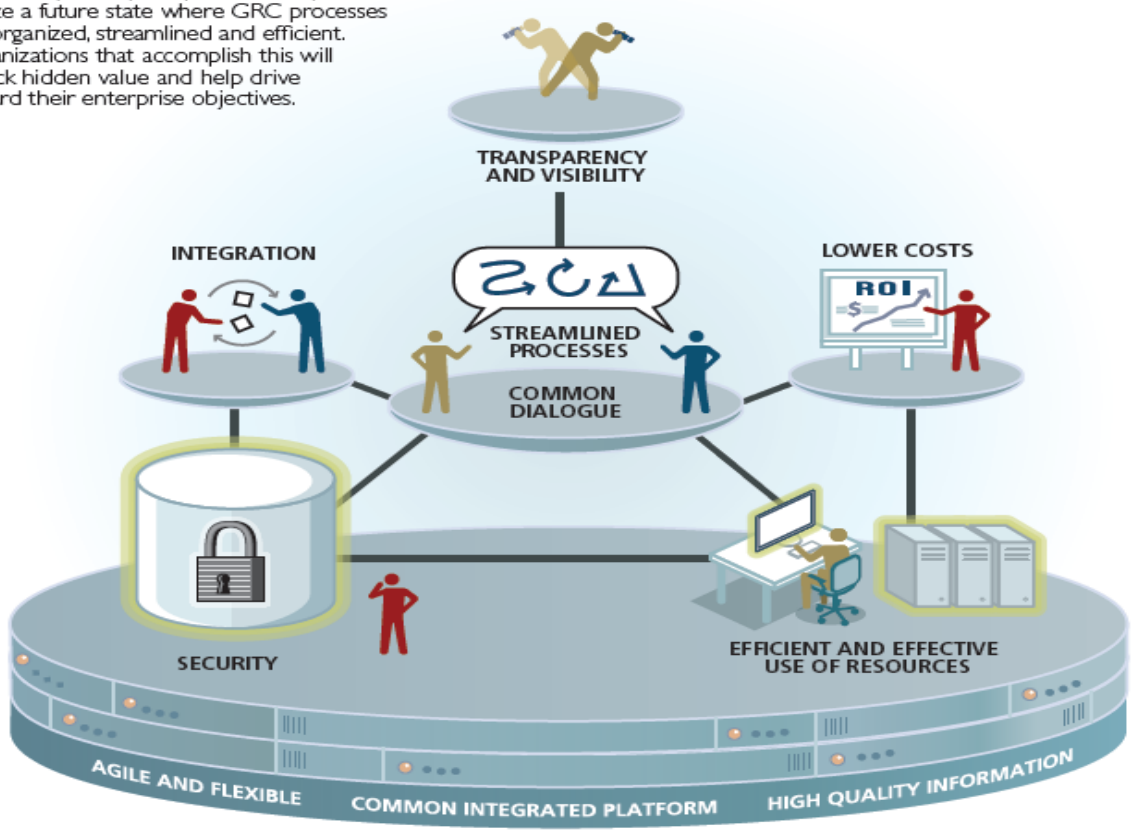
GRC 시스템의 필요성 - To-Be GRC: 통합성, 투명성, 가시성

Deloitte.

To-Be GRC 시스템은 사후통제->예방통제, 수작업->자동화, 사일로->통합, 단일솔류션->통합솔루션, 고비용->저비용 달성을 통해서 기업의 통합성, 투명성, 가시성을 향상

FUTURE STATE

As with any enterprise process, it is possible to realize a future state where GRC processes are organized, streamlined and efficient. Organizations that accomplish this will unlock hidden value and help drive toward their enterprise objectives.



Critical Success Factors

Team
Leadership alignment and the right mix of skills to see and analyze the entire situation

Openness
Willingness to listen; face the facts; don't shoot messengers

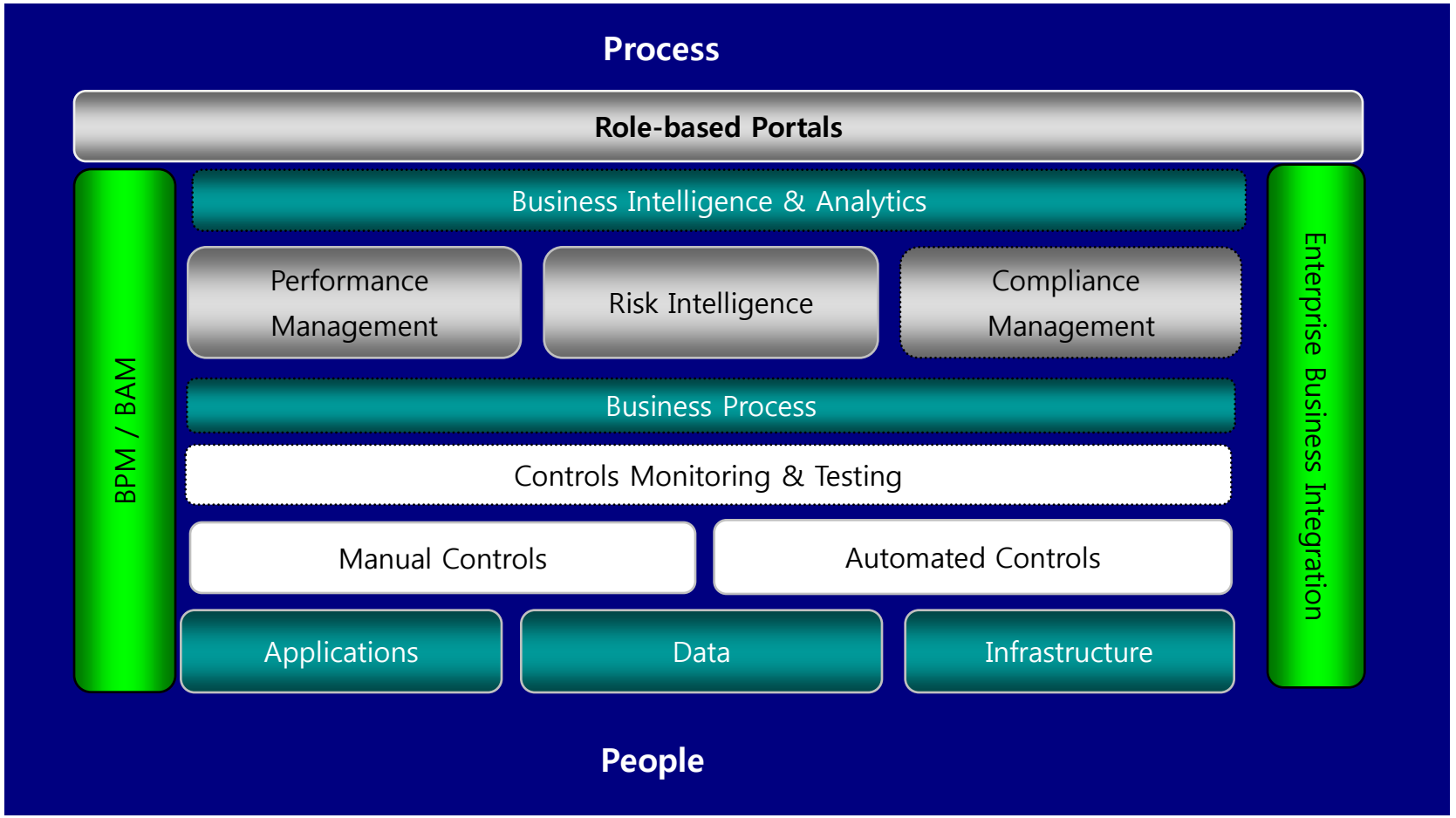
Enterprise Perspective
Get out of siloed thinking to see the big picture

Fact-Driven Analysis
Accurate, relevant information that reflects reality; use both quantitative and qualitative evidence

Clear & Compelling Story
Numbers will not speak for themselves – the numeric case must be supported by a narrative case

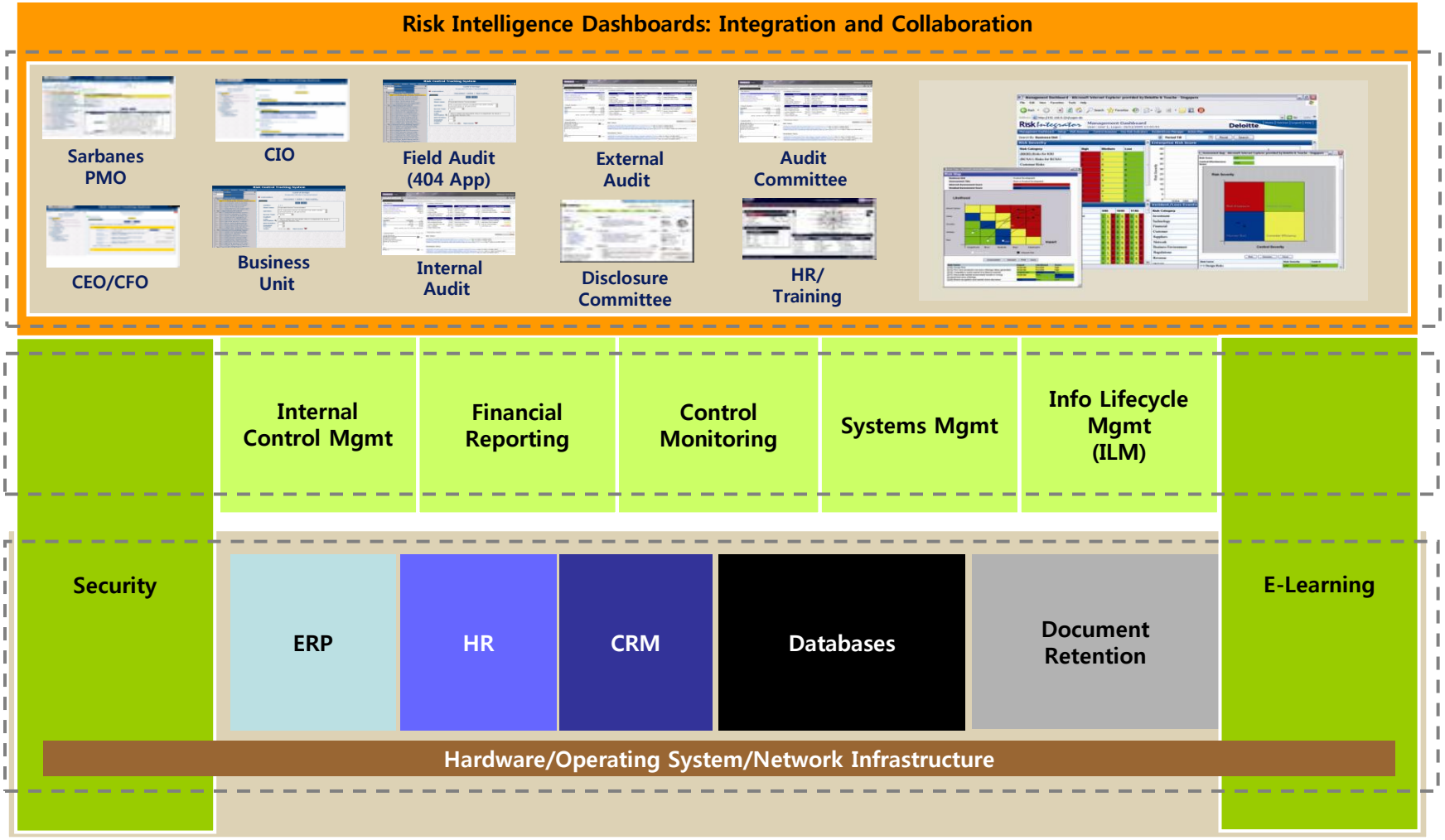
ORACLE

GRC 시스템의 필요성 - To-Be GRC: 프로세스와 성과관리 통합



GRC 시스템의 기능별 영역

Deloitte.

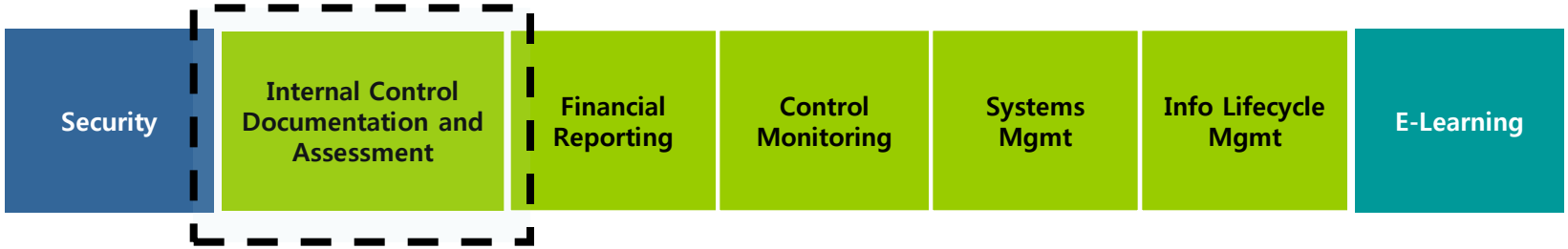


ORACLE

GRC 시스템의 기능별 영역 - 내부통제

Deloitte.

■ Reference Architecture : Internal Control Documentation and Assessment

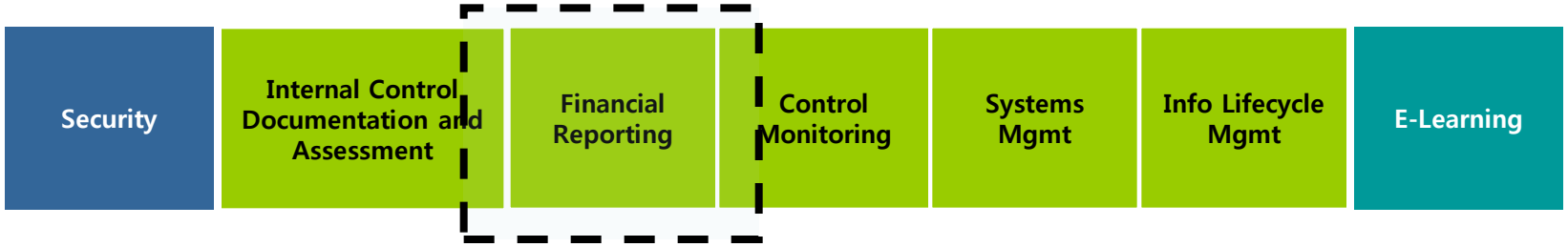


Provides sustainable environments to enable the documentation, monitoring, assessment, and reporting on internal controls on an ongoing basis

Internal Control Documentation And Assessment activities	Functionality	Associated Oracle GRC Products
Documentation	Documenting the processes relevant to Sarbanes Oxley and risks and controls for each process; identifying and documenting related policies, procedures and system documentation; template test plans for relevant controls, issue documentation and tracking	Risk & Compliance Management ▪ **GRC Manager** ▪ **Project Portfolio Management** Controls Management ▪ **Application Access Controls** ▪ **Application Configuration Controls** Access Manager Database Vault
Assessments	Risk and control assessments; evaluating design and operating effectiveness of controls; issue identification	
Testing	Documenting results of control testing; issue identification	
Reporting	Reporting by process, business unit or financial statement line i tem; status reports; deficiency reporting; dashboards, issue reporting	

GRC 시스템의 기능별 영역 – 재무분석 보고

■ Reference Architecture : Financial Reporting



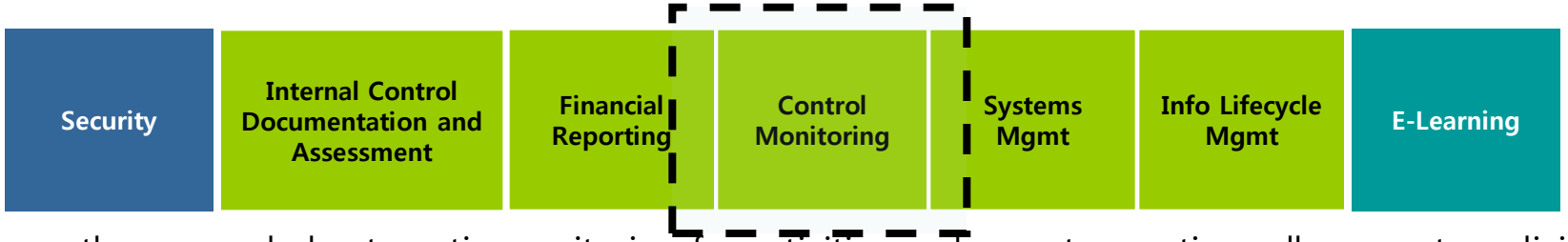
Includes the consolidated financial reporting across many systems to help in the management of financial information, consolidated reporting and the financial closing process

Financial Reporting Activit ies	Functionality	Associated Oracle GRC Products
Accounting consolidation	Inter-company eliminations, transfer pricing, foreign exchange, industry specific, tax, allocations, cash flow	Performance Management ▪ **Financial Consolidation** ▪ **Enterprise Planning & Budgeting** ▪ **Balanced Scorecard** Risk & Control Intelligence ▪ **Fusion GRC Intelligence** ▪ **Business Intelligence**
Process man agement	Workflow, consolidation, submissions, audit ability of adjustments, sign-offs	
Reporting and Disclosure	Consolidated reporting, footnote disclosures, XBRL, linkage of internal controls to financial reports	

GRC 시스템의 기능별 영역 – 통제 모니터링

Deloitte.

■ Reference Architecture : Control Monitoring



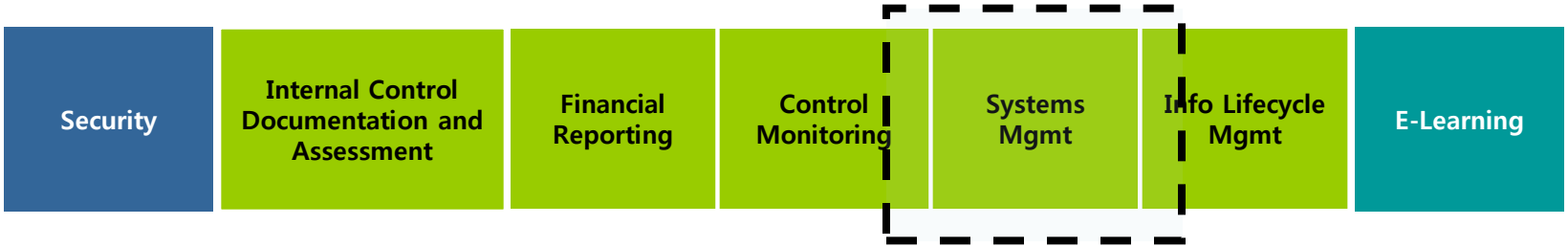
Addresses the as-needed automatic monitoring for activities such as a transaction adherence to policies and defined controls, fraud prevention, segregation of duties and changes in controls

Monitoring Activit ies	Functionality	Associated Oracle GRC Products
Changes in Control	Monitoring changes in the parameters in control configuration tables	Operational Intelligence ▪ **BPEL Process Manager** ▪ **Business Activity Monitoring** Data Audit ▪ **Audit Vault** GRC Manager Controls Management ▪ **Application Access Controls** ▪ **Application Configuration Controls** Identity & Access Management ▪ **Access Manager** ▪ **Identity Manager** ▪ **Enterprise Single Sign-on** ▪ **Virtual Directory**
Segregation of Duties & User Access	Ability to know wh o has access to various transactions and/or modules; an access matrix for defining incompatible transactions/functions; monitoring access tables for potential access conflicts; monitoring who has accessed transactions, modules and content	
Transaction Monitoring	Analyzing transactions for anomalies outside the parameters of controls, monitoring for completeness and accuracy transactions and other unusual transactions outside tolerance levels	
Process Monitoring	Monitoring manual process such as reconciliations, periodic closing compliance certifications	

GRC 시스템의 기능별 영역 – 변경 관리

Deloitte.

■ Reference Architecture : Systems Mgmt.



Addresses repeatable IT process execution and the real-time status and management of IT infrastructure assets underlying a company's financial systems

Systems Management Activities	Functionality	Associated Oracle GRC Products
Configuration Management	Identify and define configuration items; monitor status of configuration items; approval process for accepting and/or modifying change requests	Change Management ▪ **Enterprise Manager**
Change & Release Management	Introducing new or changed configuration items to the infrastructure; promoting software and hardware into production	
Incident & Problem Management	Documentation and resolution of inc idents, restore services to minimize service disruption, logging, trouble tickets, communications	
Availability Management	Ensure services are available to the customer at the level defined by the service level agreement, s ervice availability, monitoring infrastructure enhancements	

ORACLE

GRC 시스템의 기능별 영역 – 정보 자산 관리

Deloitte.

■ Reference Architecture : Info Lifecycle Mgmt

Addresses the critical components of Sarbanes Oxley as it relates to document retention and enterprise content management including the processes, procedures and technology to manage and archive data

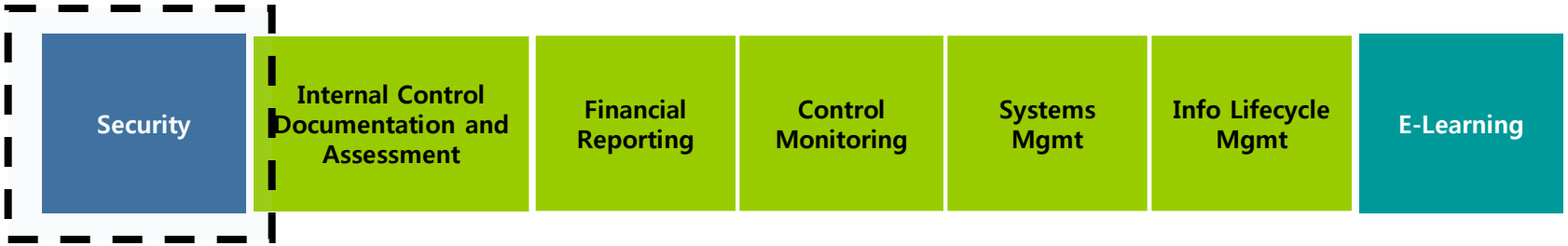
Information Lifecycle Management activities	Functionality	Associated Oracle GRC Products
Document Management and Retention	Document Management and Retention policies; document capture, classification, tracking, and retention management	Content Management ▪ **Universal Content Management** ▪ **Universal Records Management** ▪ **Content Database** ▪ **Records Database** ▪ **Information Rights Management**
Records Disposal	E-mail and document elimination per policies; tracking	
Information Classification	Taxonomy to classify documentation, category maintenance documents, recovery by classification	

ORACLE

GRC 시스템의 기능별 영역 – 접근 통제, SOD

Deloitte.

■ Reference Architecture : Security



Addresses the protection of financial information. It provides for secure access to information and applications, Segregation of Duties, and auditing of access

Security Activities	Functionality	Associated Oracle GRC Products
Configuration Management of Security and Controls	Base configuration parameters; periodic evaluation and improvements of security and control parameters; applicable to platform, middleware and application	Identity & Access Management ▪ **Access Manager** ▪ **Identity Manager** ▪ **Enterprise Single Sign-on** ▪ **Virtual Directory** Data Security ▪ **Database Vault** ▪ **Label Security** ▪ **Advanced Security** ▪ **Secure Enterprise Search** Controls Management ▪ **Application Access Controls** ▪ **Application Configuration Controls**
Segregation of Duties and User Access	Establishing segregation of duties matrix; identifying appropriate roles for users; managing user access to infrastructure, applications and content	
Network Infrastructure Security	Firewal ls, anti -spam, anti -virus, intrusion detection, incident response	
Safeguarding Assets	Appropriate physical restrictions to critical infrastructure, applications and content	

ORACLE

GRC 시스템의 기능별 영역 – 절차 및 규정 관리

Deloitte.

■ Reference Architecture : e-Learning

Addresses training documentation as it relates to Sarbanes-Oxley Compliance. Organizations need to provide credible documentation that key staff have been trained on compliance requirements.

E -Learning Activit ies	Functionality	Associated Oracle GRC Products
Documentation and Content Management	Creating content, publishing to e-Learning system, managing and archiving content	Policy Management ▪ **Learning Management** ▪ **Policy & Procedure Portal**
Delivering Training	End -user interface to access, participate and complete the training; learning management systems	
Tracking Participation	Documentation on who has completed the training and when	

ORACLE

GRC 시스템의 기능별 영역 – 통합 감사

Deloitte.

■ Reference Architecture : Integration and Collaboration

Integration and Collaboration

Enables efficient the processes and interfaces that support continuous monitoring and control

Integration and Collaboration Activities	Functionality	Associated Oracle GRC Products
User Interaction	Access, review and input information; web-based interface applications; integrated portal; customized views based on user; reporting	Risk & Control Intelligence ▪ **Fusion GRC Intelligence** ▪ **Business Intelligence** Operational Intelligence ▪ **BPEL Process Manager** ▪ **Business Activity Monitoring** **GRC Manager** Data Audit ▪ **Audit Vault**
Process Integration	Process correlation, workflow, routing	
Data Integration	Validate data, transform data, data quality	
Application Connectivity	Integrate multiple applications, messaging between applications	

GRC 의 효과 – 내부적

Deloitte.

☑ **통합 관리**
- 성과, 리스크, 법규 준수에 대한 통합된 관리를 통하여 기업의 각각의 이해 당사자들의 요구사항의 균형을 맞추도록 전사적인 대응 용이

☑ **리스크 관리 혁신**
- 기업의 주요 프로세스와 의사결정 과정에 통합된 GRC를 통해 기업은 가치에 기반한 경영계획 수립을 위한 양질의 정보, 리스크를 고려한 의사결정과 실현 가능한 전략 수립 지원

☑ **비용 절감**
- 프로세스와 통제 자동화 및 통합을 달성하는 것은 곧 중복된 노력 및 인적자원 사용의 방지, 에러 발생 가능성이 높은 수작업의 감소, 비용발생을 야기하는 재 작업의 감소를 의미
- 또한 외부 감사, 내부 감사 등 내 외부 감사로 인한 비용을 절감

☑ **비즈니스 성과 극대화**
- 통합된 의사결정, 향상된 리스크 관리, 비용 감소를 통해서 전략적인 목표를 위해 더 많은 자원을 투입할 수 있게 하는 효과
- 양질의 정보를 기반으로 경영진은 더 확고한 전략적 의사 결정을 내리고 실행할 수 있으며, 이는 궁극적으로 투자자들의 확신을 증대시킴

☑ **글로벌 표준**
- 시장 통합과 글로벌 경쟁력에 맞는 표준
- 국제 회계 기준 적용에 따른 리스트 관리 및 통제 관리 시스템의 표준

GRC 의 효과 - 외부적

Deloitte.

기업 경쟁력 강화	투명성, 신뢰성 제공	통제수준 향상
• 전략 및 기업의 주요 성과/위험 지표 및 한도/목표를 설정하고 이의 초과여부 및 조기경보를 위한 지표의 변화 모니터링 • 경영자에 주기적으로 보고하고 이상징후 발견 시 신속한 대응	• 독립적인 위험관리 조직의 운영을 통해 기업의 이해관계자의 기업지배에 관한 투명성 제고 • 대외 보고서 등에 기업의 Risk Profile과 이의 관리 현황을 보고하여 투자자에게 긍정적 신뢰 제공	• 체계적이고 전반적인 전략에 따른 통제 및 위험관리 투자를 통해 중복투자 방지 및 비용 시너지 효과 • 체계적인 위험 및 위험 관리로 위험 관리 프로세스의 효율성 제고

중점적인 위험 관리 분야

접근보안	프로세스	환경 및 안전	위험 및 재난관리

ORACLE

GRC 성숙도 모델 – GRC 비전을 향한 여정

Deloitte.

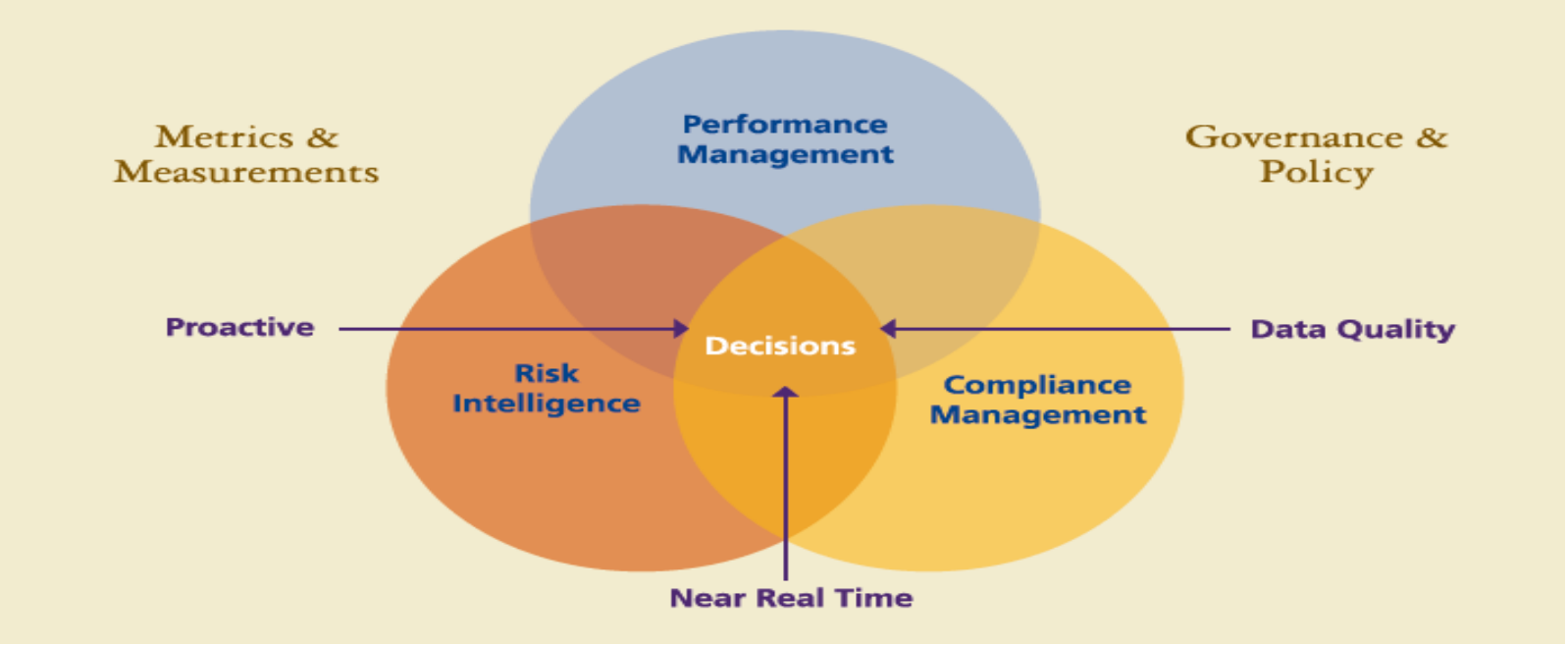
GRC 부재	스프레드 쉬트 기반의 GRC	GRC의 자동화	지속 가능한 GRC	GRC 비전
-가시성 부족 -업무 유관성 부족 -사후 대응 중심의 통합되지 않은 접근 방식 -불필요한 반복 작업	-위험 중심이 아닌 접근 방법 -중복 통제 -수작업을 통한 업무/IT 프로세스 및 통제 -비효율적이며 노동 집약적인 테스트 -통제 상의 이슈 발생 시 사후 대처 적인 접근 방식	-어플리케이션 기반 업무/IT 프로세스 통제 -효과적인 통제의 운영 및 테스트 - 자동화된 테스트 능력 -사용자 접근 통제 및 업무 분장 수립 -통제의 합리화	-효과적인 통제의 운영 -통제 이슈에 대한 예방적인 접근 -검증된 통제의 운영 -지속적인 규제 준수 프로세스 -투자대비 효과(ROI)/비즈니스적인 가치 추구	-거버넌스의 정착 -효율적이고 유연한 통제의 운영 -기업의 사회적 책임 준수 -투자자들의 확신 제고 -위험요소의 보완 및 분석 -비즈니스 성과 및 지속성 개선
혼란상태	수작업	자동화	모니터링	가치실현

KR

ORACLE

결론 - 성공적인 GRC 추진 전략

- 전략: 전사적인 전략과 통합된 GRC 의 범위 및 목표 설정(ROI,KPI 등)
- 진단: 전사적 GRC 대응 수준 및 체계 진단
- 설계: 비즈니스 요구 사항의 정확한 도출 (법규적, 관리적, 기술적 측면)
- 단계: 단계별 실행 계획 수립 (Access Control, IDM 등 기본적인 것부터 수행)
- 전문가: 전략 수립 및 설계 시 정보시스템, 프로세스, 감사/통제 전문가의 참여
- 솔루션: 회사의 전략과 환경에 적합한 Solution 및 기술의 선정 및 통합




Deloitte.