LES DOCUMENTS ET OUTILS OFFERTS PAR ISACA EN MATIÈRE DE GIA

Symposium GIA - 28 février 2017, Québec

David Henrard, CISA, CISM, CRISC, COBIT5 Implementation & Assessor

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

GIA SYMPOSIUM QUÉBEC 2017
GESTION DES IDENTITÉS ET DES ACCÈS

levio
AFFAIRES ET TECHNOLOGIES

ISACA en résumé

- Une communauté de 140 000 professionnels présente dans 180 pays

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

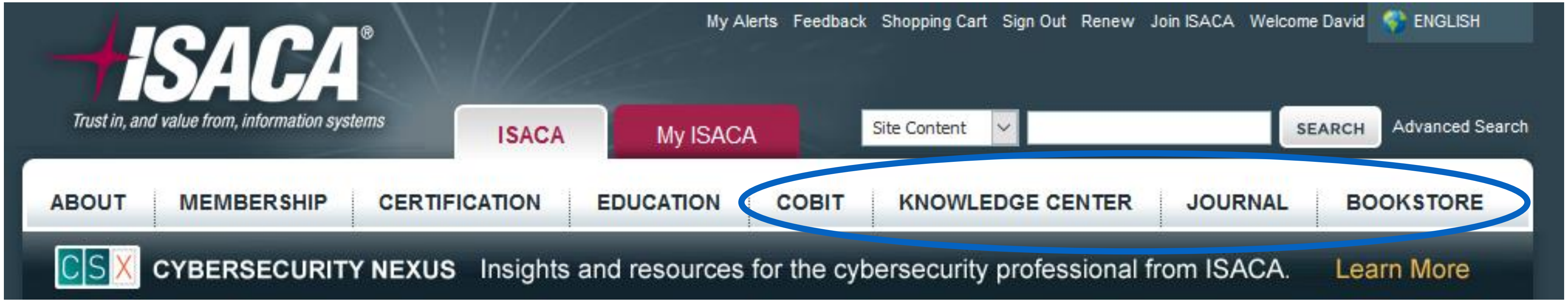
CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

COBIT® 5
AN ISACA® FRAMEWORK

CSX™
CYBERSECURITY NEXUS

Le site internet d'ISACA www.isaca.org



My Alerts Feedback Shopping Cart Sign Out Renew Join ISACA Welcome David ENGLISH

ISACA® Trust in, and value from, information systems

ISACA My ISACA

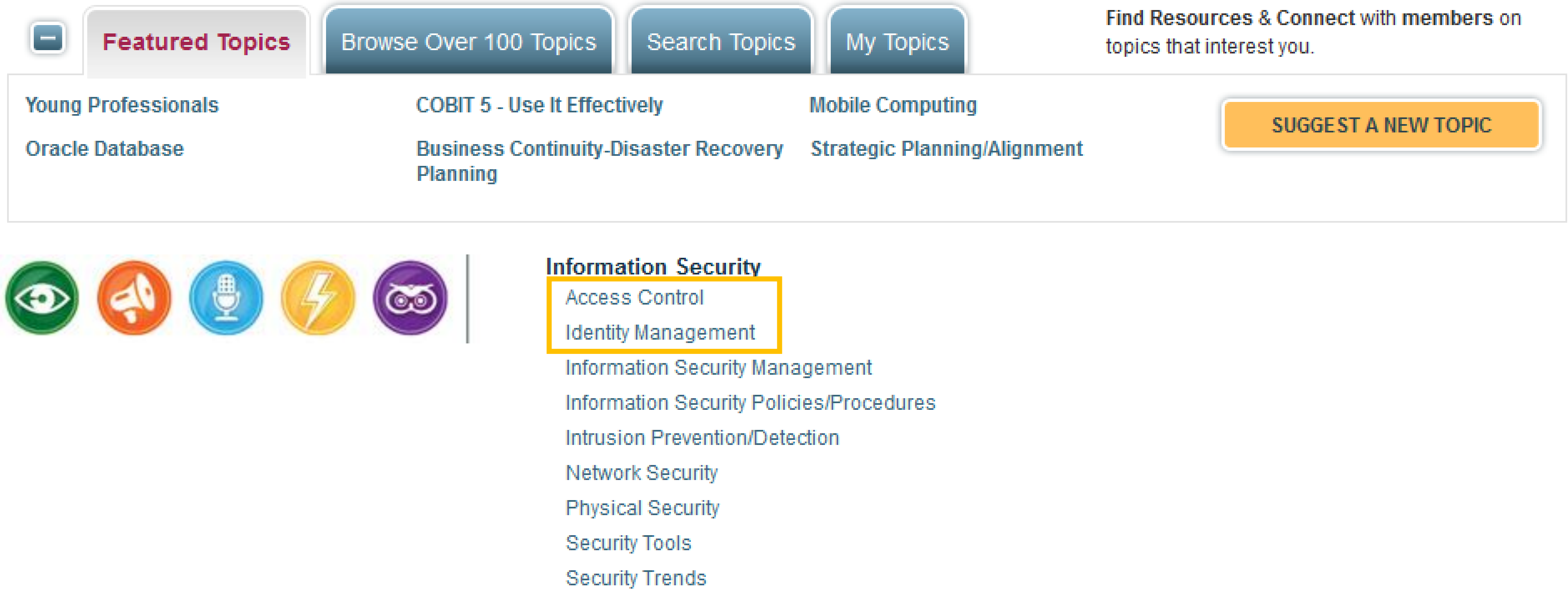
Site Content SEARCH Advanced Search

ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE CENTER JOURNAL BOOKSTORE

CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA. Learn More

Knowledge Center

- IT Professional Networking and Knowledge Center



Find Resources & Connect with members on topics that interest you.

Young Professionals

Oracle Database

COBIT 5 - Use It Effectively

Business Continuity-Disaster Recovery Planning

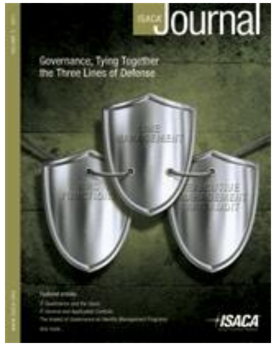
Mobile Computing

Strategic Planning/Alignment

Information Security

- Access Control
- Identity Management
- Information Security Management
- Information Security Policies/Procedures
- Intrusion Prevention/Detection
- Network Security
- Physical Security
- Security Tools
- Security Trends

The Impact of Governance on Identity Management Programs



Volume 5 , 2011

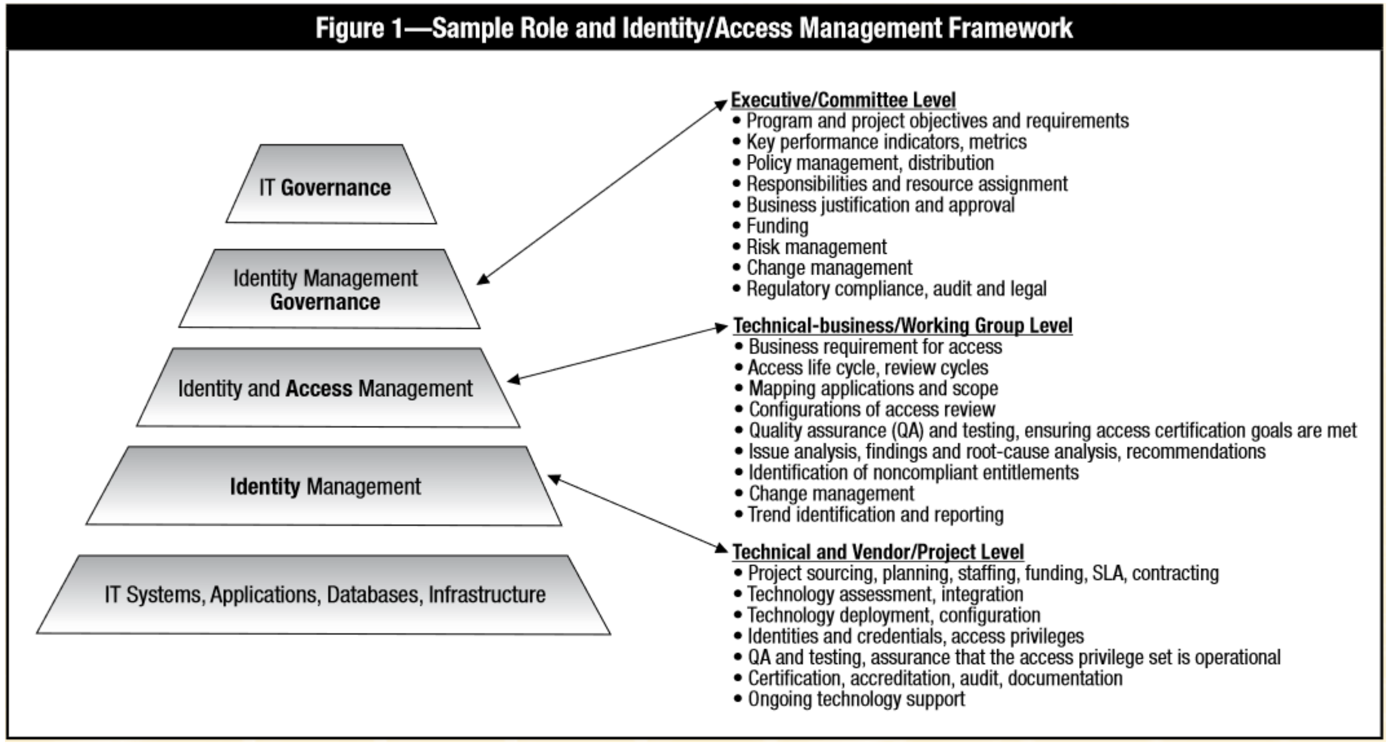


Figure 1—Sample Role and Identity/Access Management Framework

IT Governance
Identity Management Governance
Identity and Access Management
Identity Management
IT Systems, Applications, Databases, Infrastructure

Executive/Committee Level

- Program and project objectives and requirements
- Key performance indicators, metrics
- Policy management, distribution
- Responsibilities and resource assignment
- Business justification and approval
- Funding
- Risk management
- Change management
- Regulatory compliance, audit and legal

Technical-business/Working Group Level

- Business requirement for access
- Access life cycle, review cycles
- Mapping applications and scope
- Configurations of access review
- Quality assurance (QA) and testing, ensuring access certification goals are met
- Issue analysis, findings and root-cause analysis, recommendations
- Identification of noncompliant entitlements
- Change management
- Trend identification and reporting

Technical and Vendor/Project Level

- Project sourcing, planning, staffing, funding, SLA, contracting
- Technology assessment, integration
- Technology deployment, configuration
- Identities and credentials, access privileges
- QA and testing, assurance that the access privilege set is operational
- Certification, accreditation, audit, documentation
- Ongoing technology support

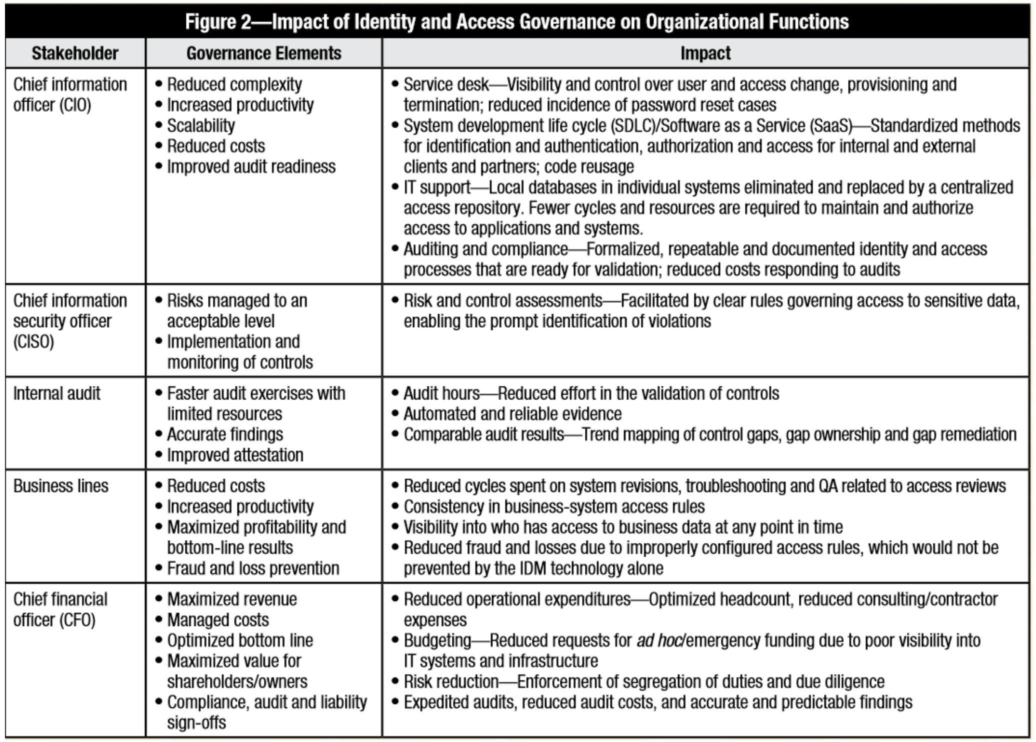
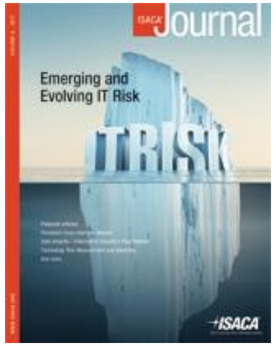


Figure 2—Impact of Identity and Access Governance on Organizational Functions

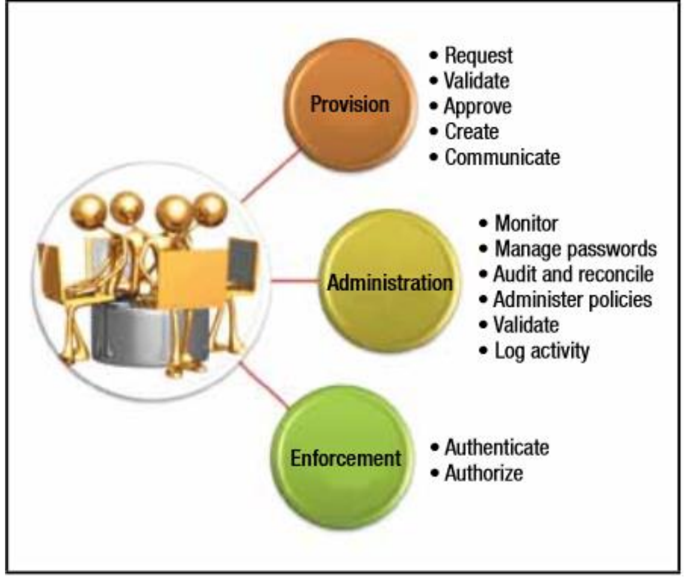
Stakeholder	Governance Elements	Impact
Chief information officer (CIO)	• Reduced complexity • Increased productivity • Scalability • Reduced costs • Improved audit readiness	• Service desk—Visibility and control over user and access change, provisioning and termination; reduced incidence of password reset cases • System development life cycle (SDLC)/Software as a Service (SaaS)—Standardized methods for identification and authentication, authorization and access for internal and external clients and partners; code reusage • IT support—Local databases in individual systems eliminated and replaced by a centralized access repository. Fewer cycles and resources are required to maintain and authorize access to applications and systems. • Auditing and compliance—Formalized, repeatable and documented identity and access processes that are ready for validation; reduced costs responding to audits
Chief information security officer (CISO)	• Risks managed to an acceptable level • Implementation and monitoring of controls	• Risk and control assessments—Facilitated by clear rules governing access to sensitive data, enabling the prompt identification of violations
Internal audit	• Faster audit exercises with limited resources • Accurate findings • Improved attestation	• Audit hours—Reduced effort in the validation of controls • Automated and reliable evidence • Comparable audit results—Trend mapping of control gaps, gap ownership and gap remediation
Business lines	• Reduced costs • Increased productivity • Maximized profitability and bottom-line results • Fraud and loss prevention	• Reduced cycles spent on system revisions, troubleshooting and QA related to access reviews • Consistency in business-system access rules • Visibility into who has access to business data at any point in time • Reduced fraud and losses due to improperly configured access rules, which would not be prevented by the IDM technology alone
Chief financial officer (CFO)	• Maximized revenue • Managed costs • Optimized bottom line • Maximized value for shareholders/owners • Compliance, audit and liability sign-offs	• Reduced operational expenditures—Optimized headcount, reduced consulting/contractor expenses • Budgeting—Reduced requests for *ad hoc*/emergency funding due to poor visibility into IT systems and infrastructure • Risk reduction—Enforcement of segregation of duties and due diligence • Expedited audits, reduced audit costs, and accurate and predictable findings

Identity and Access Management - Its Role in Sarbanes-Oxley Compliance



Volume 6 , 2011

Figure 2—Stages for an IAM System



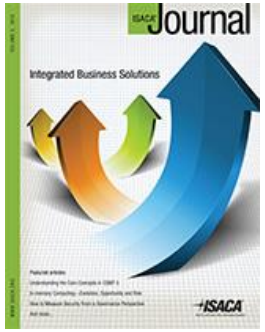
Provision
- Request
- Validate
- Approve
- Create
- Communicate

Administration
- Monitor
- Manage passwords
- Audit and reconcile
- Administer policies
- Validate
- Log activity

Enforcement
- Authenticate
- Authorize

ISACA Journal

Solving the Identity and Access Management Conundrum



Volume 5 , 2013

Figure 1—Benefits Realization Through a Phased Road Map

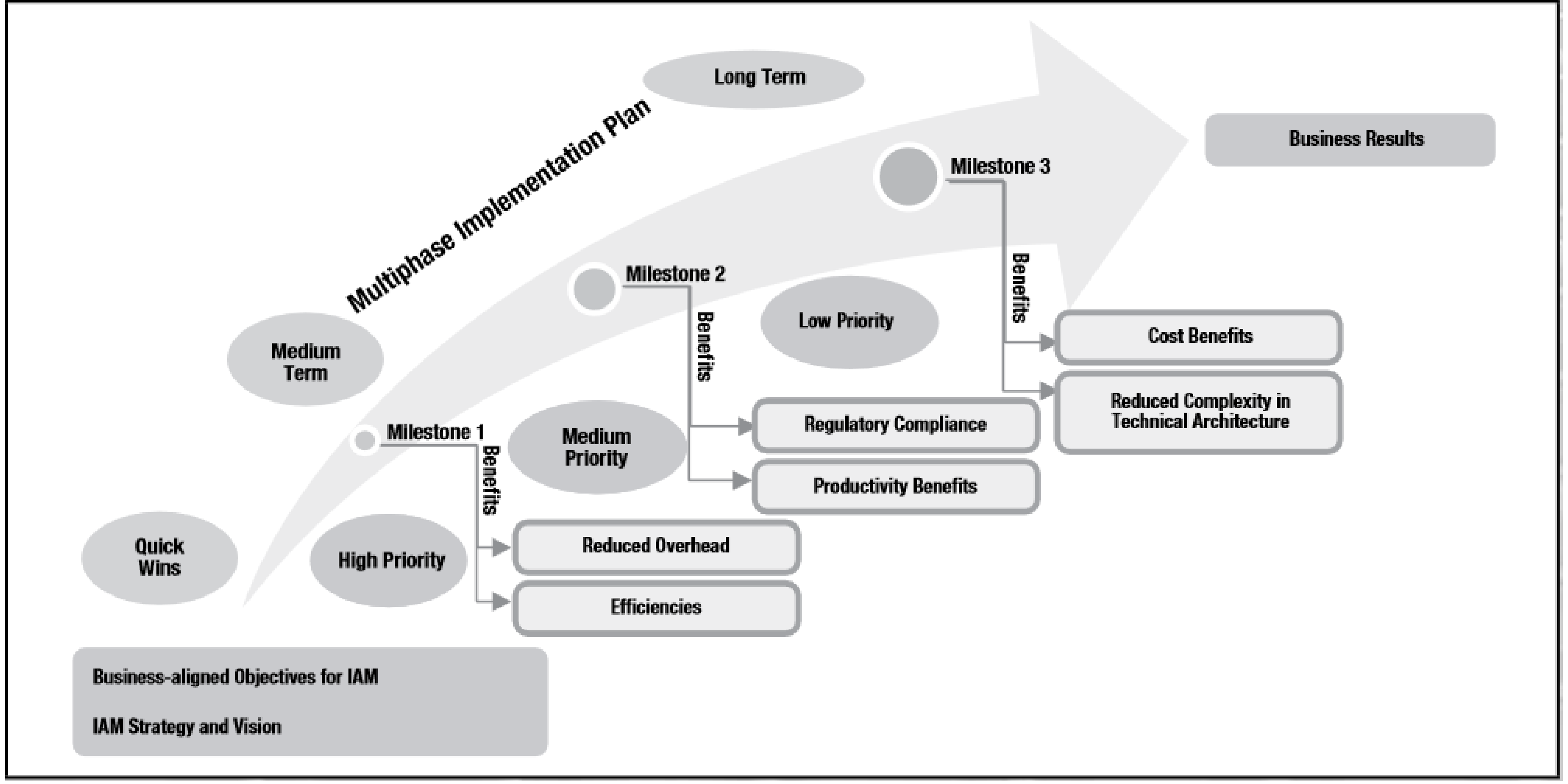
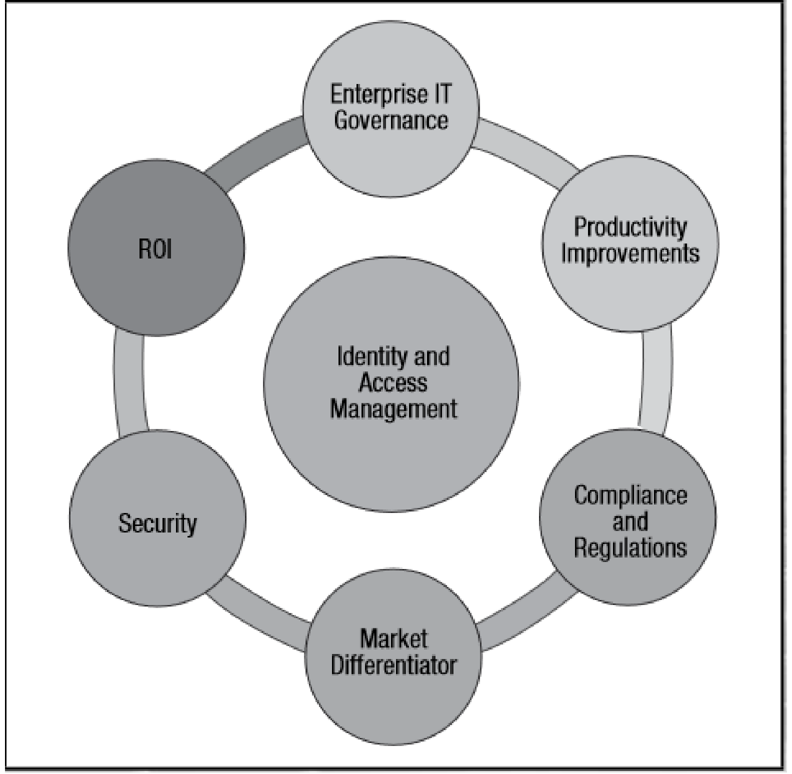


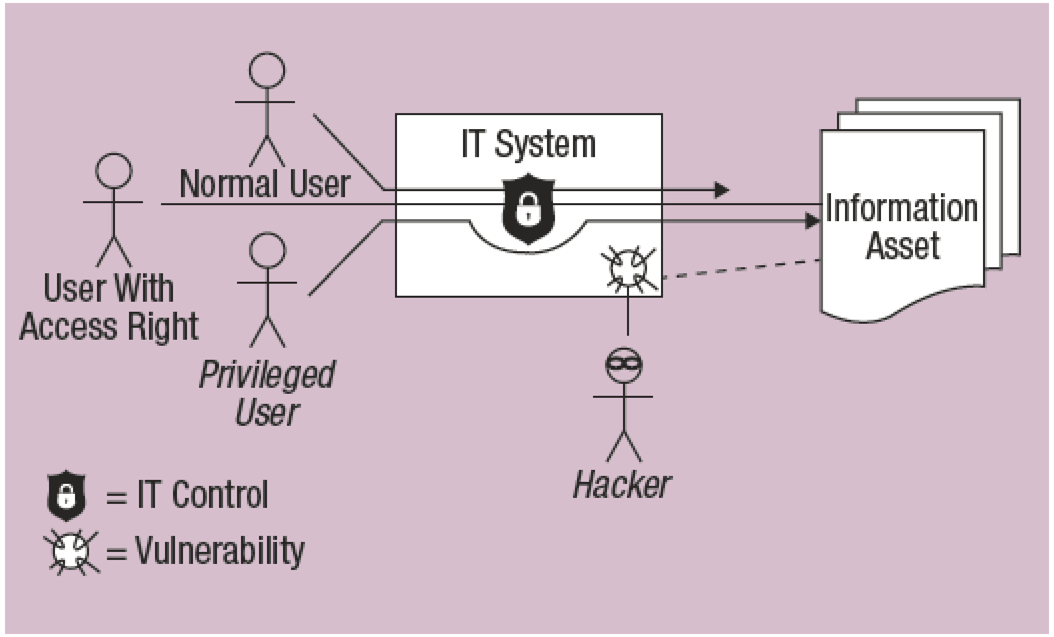
Figure 2—IAM Target Goals


Enterprise IT Governance
ROI
Productivity Improvements
Identity and Access Management
Security
Compliance and Regulations
Market Differentiator

Capability Framework for Privileged Access Management

Volume 1 , 2017

Figure 1—Distinguishing Privileged Access From Regular Access to Information Assets



Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

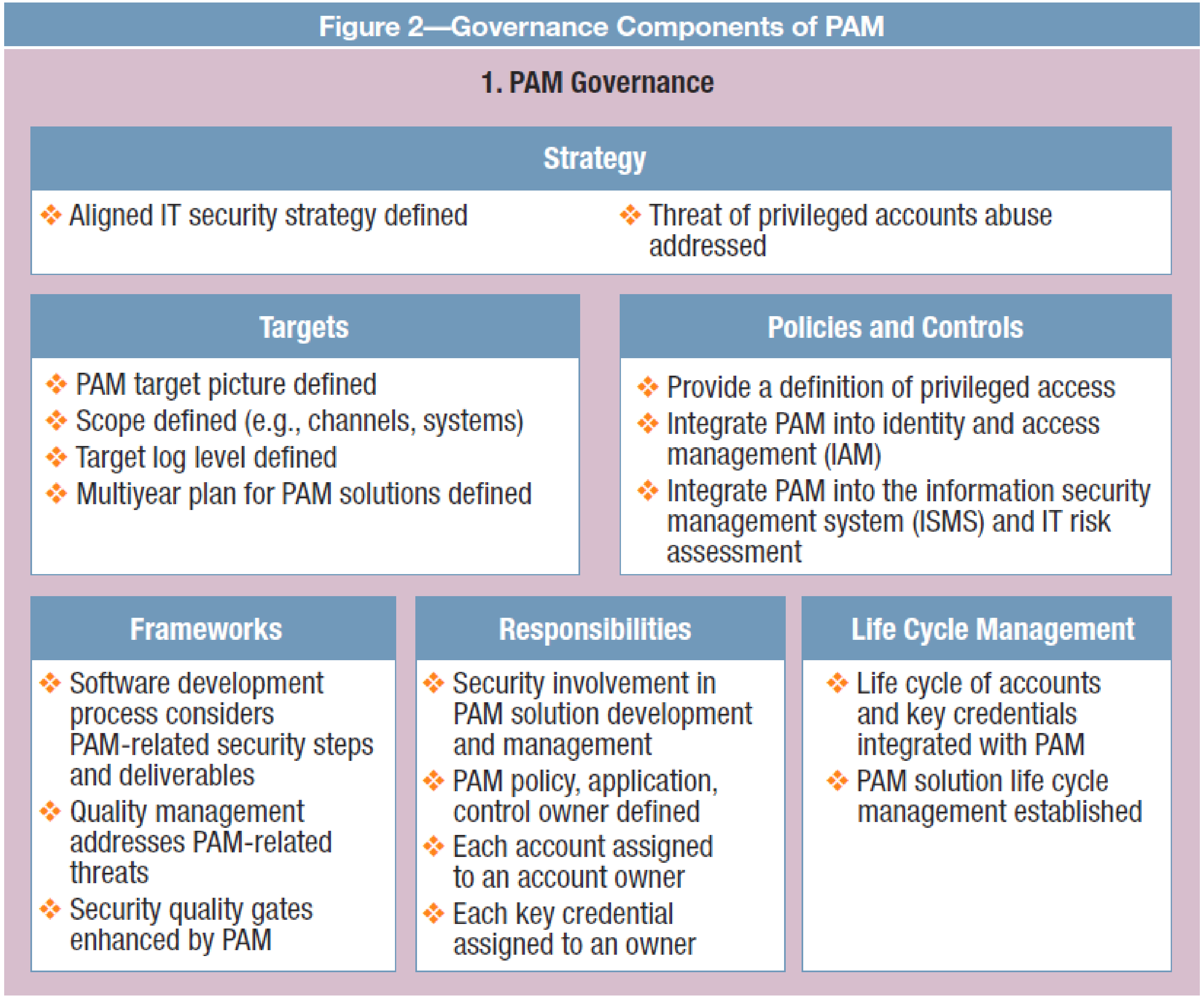


Figure 2—Governance Components of PAM

1. PAM Governance

Strategy

- Aligned IT security strategy defined
- Threat of privileged accounts abuse addressed

Targets

- PAM target picture defined
- Scope defined (e.g., channels, systems)
- Target log level defined
- Multiyear plan for PAM solutions defined

Policies and Controls

- Provide a definition of privileged access
- Integrate PAM into identity and access management (IAM)
- Integrate PAM into the information security management system (ISMS) and IT risk assessment

Frameworks

- Software development process considers PAM-related security steps and deliverables
- Quality management addresses PAM-related threats
- Security quality gates enhanced by PAM

Responsibilities

- Security involvement in PAM solution development and management
- PAM policy, application, control owner defined
- Each account assigned to an account owner
- Each key credential assigned to an owner

Life Cycle Management

- Life cycle of accounts and key credentials integrated with PAM
- PAM solution life cycle management established

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

Volume 1 , 2017

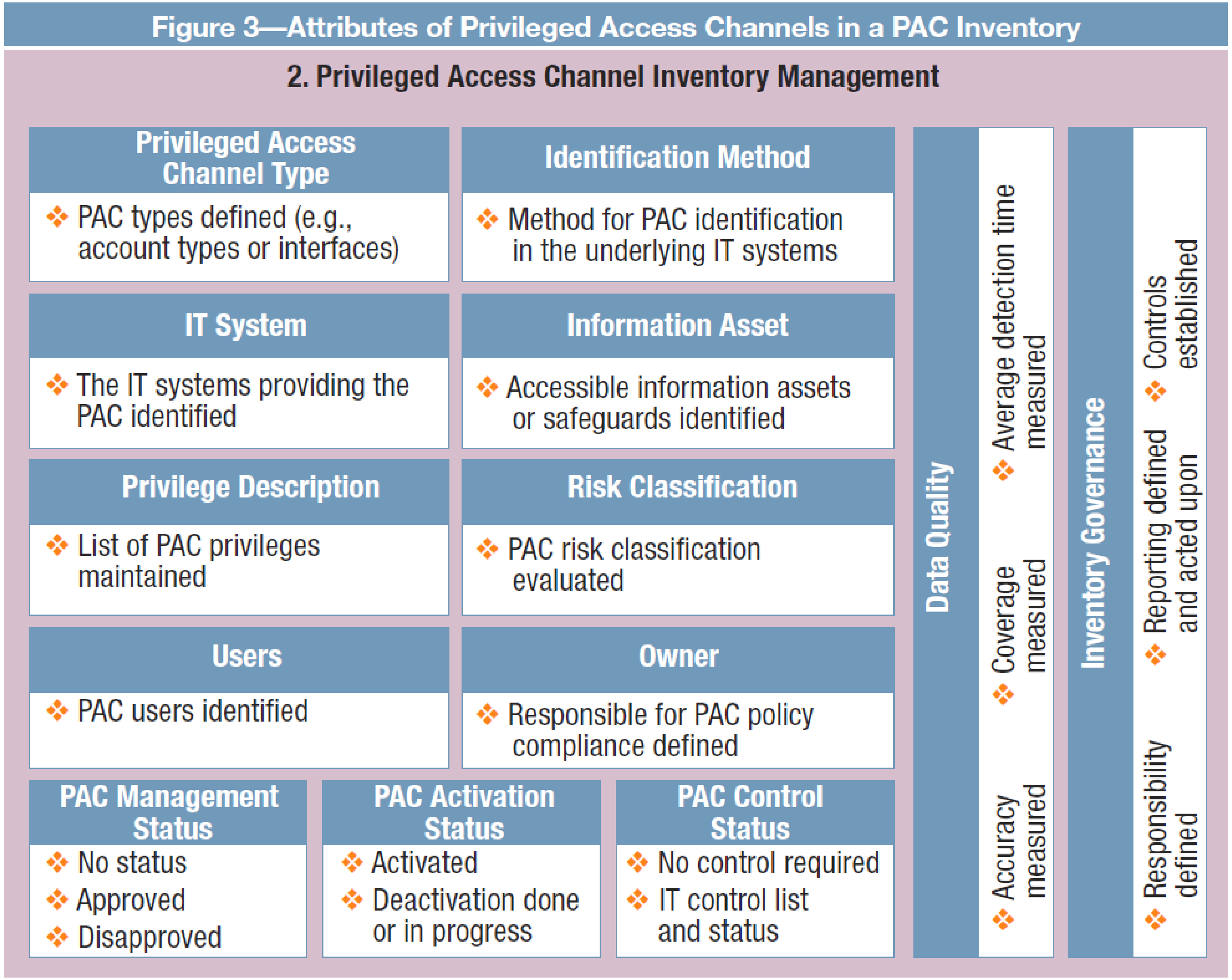


Figure 3—Attributes of Privileged Access Channels in a PAC Inventory

2. Privileged Access Channel Inventory Management

Privileged Access Channel Type
- PAC types defined (e.g., account types or interfaces)

Identification Method
- Method for PAC identification in the underlying IT systems

IT System
- The IT systems providing the PAC identified

Information Asset
- Accessible information assets or safeguards identified

Privilege Description
- List of PAC privileges maintained

Risk Classification
- PAC risk classification evaluated

Users
- PAC users identified

Owner
- Responsible for PAC policy compliance defined

PAC Management Status
- No status
- Approved
- Disapproved

PAC Activation Status
- Activated
- Deactivation done or in progress

PAC Control Status
- No control required
- IT control list and status

Data Quality
- Accuracy measured
- Coverage measured
- Average detection time measured

Inventory Governance
- Responsibility defined
- Reporting defined and acted upon
- Controls established

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

Volume 1 , 2017

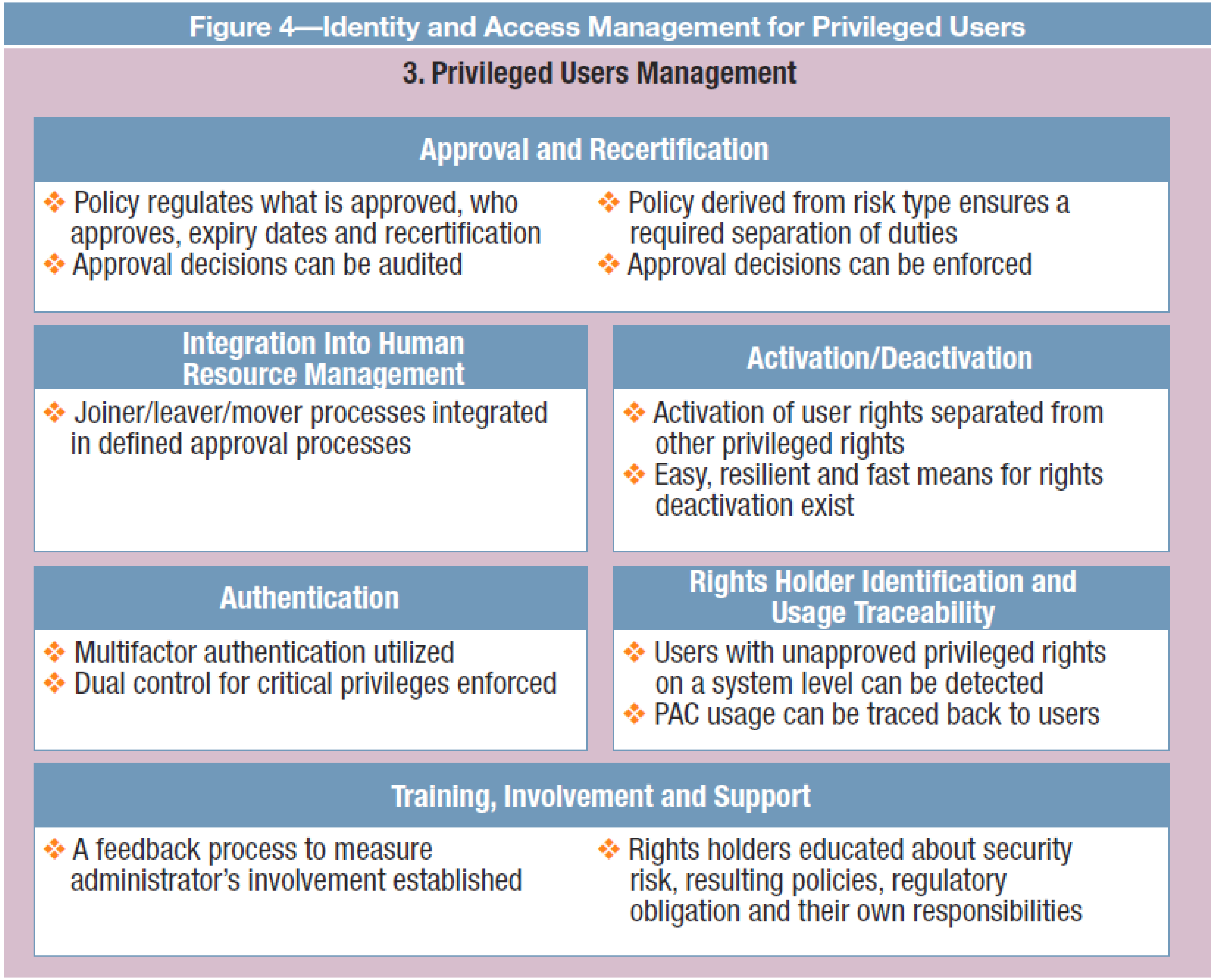


Figure 4—Identity and Access Management for Privileged Users

3. Privileged Users Management

Approval and Recertification

- Policy regulates what is approved, who approves, expiry dates and recertification
- Approval decisions can be audited
- Policy derived from risk type ensures a required separation of duties
- Approval decisions can be enforced

Integration Into Human Resource Management

- Joiner/leaver/mover processes integrated in defined approval processes

Activation/Deactivation

- Activation of user rights separated from other privileged rights
- Easy, resilient and fast means for rights deactivation exist

Authentication

- Multifactor authentication utilized
- Dual control for critical privileges enforced

Rights Holder Identification and Usage Traceability

- Users with unapproved privileged rights on a system level can be detected
- PAC usage can be traced back to users

Training, Involvement and Support

- A feedback process to measure administrator's involvement established
- Rights holders educated about security risk, resulting policies, regulatory obligation and their own responsibilities

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

Volume 1 , 2017

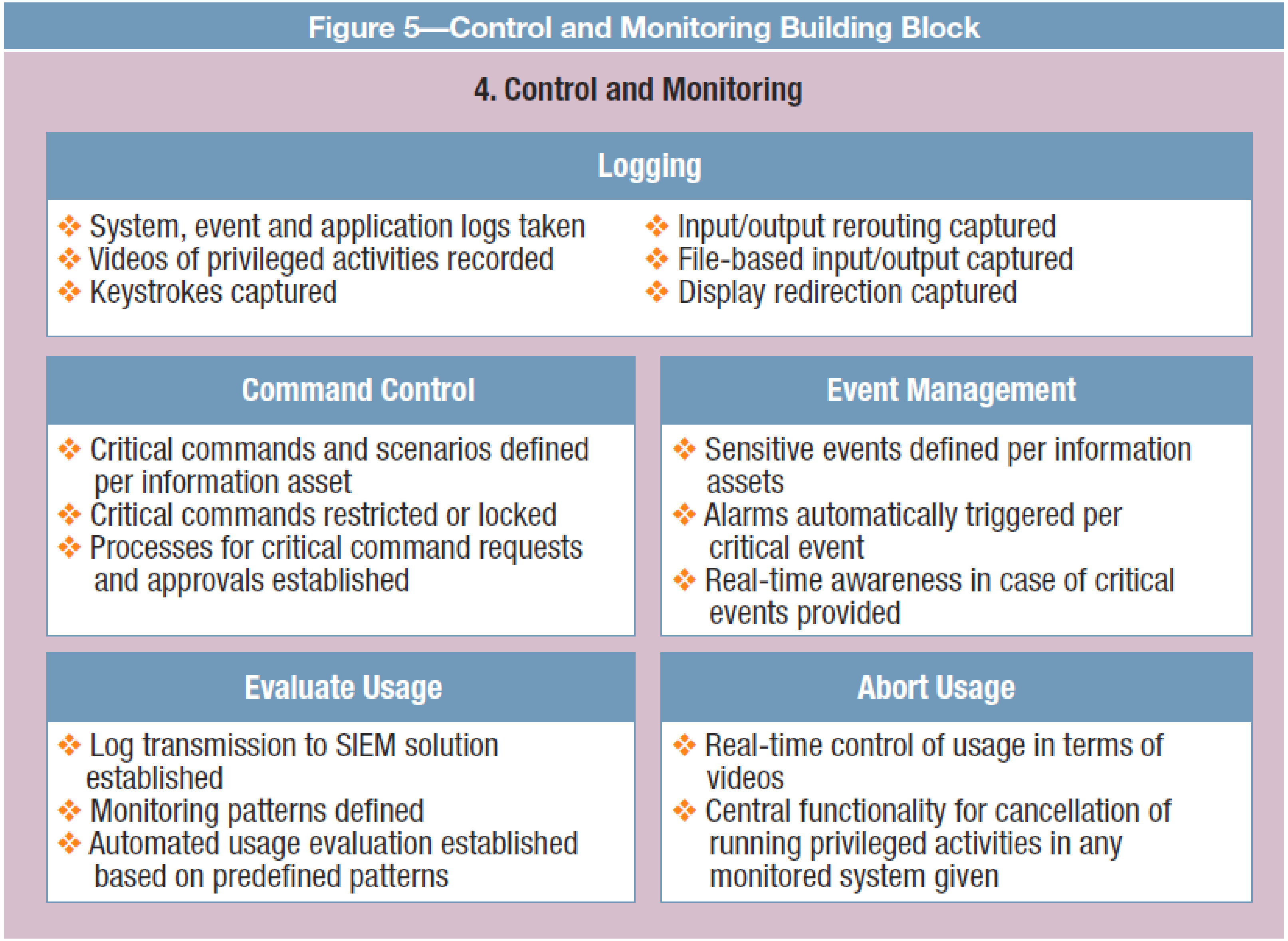


Figure 5—Control and Monitoring Building Block

4. Control and Monitoring

Logging

- System, event and application logs taken
- Videos of privileged activities recorded
- Keystrokes captured
- Input/output rerouting captured
- File-based input/output captured
- Display redirection captured

Command Control

- Critical commands and scenarios defined per information asset
- Critical commands restricted or locked
- Processes for critical command requests and approvals established

Event Management

- Sensitive events defined per information assets
- Alarms automatically triggered per critical event
- Real-time awareness in case of critical events provided

Evaluate Usage

- Log transmission to SIEM solution established
- Monitoring patterns defined
- Automated usage evaluation established based on predefined patterns

Abort Usage

- Real-time control of usage in terms of videos
- Central functionality for cancellation of running privileged activities in any monitored system given

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

Volume 1 , 2017

Merci !

David Henrard, CISA, CISM, CRISC, COBIT5 Implementation & Assessor
Responsable de la pratique « Sécurité »
Conseiller senior en sécurité de l’information, PRP et gouvernance des TI
david.henrard@levio.ca