IT RISK REGISTER

Getachew T.

EDUCAUSE IT GOVERNANCE, RISK, AND COMPLIANCE PROGRAM

Risk-Based Audits

Risk-based audits also use industry frameworks to ascertain support of organizational goals and conformance to external parameters. In contrast to compliance-based audits, they also apply the enterprise's risk appetite, risk tolerance and expectation of compliance. Risk appetite is the level of risk the enterprise is willing to accept in pursuit of its goals, objectives and mission and how much deviation is tolerable. First, IT auditors should consult senior management to establish risk thresholds. Then the auditors should involve subject matter experts to guarantee the accurate interpretation and employment of technical controls. At the strategic level, auditors should discuss risk factors that impact the enterprise's mission, vision, strategy and objectives.

Risk-based internal auditing is driven by the most recent risk assessments, with the top threats being covered first and far more frequently. It ensures that the internal audit activity is focusing its efforts on providing assurance and advisory services related to the organization's top risks.

Compliance-Based Audits

Compliance-based audits evaluate compliance with laws, regulations and internal policies. These audits are necessary to establish a reasonable level of assurance that an enterprise is conforming with external requirements and internal processes. The risk of noncompliance, such as fees and penalties, necessitates compliance with industry standards and recognized practices. Compliance-focused audits use frameworks such as those created by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) to support enterprise objectives and comply with external requirements.

IT Risk Register

The Risk Register is the document containing the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. The risk register details all identified risks, including description, category, cause, probability of occurring, impact on objectives, proposed responses, owners, and current status. It is a spreadsheet containing all the statements of risk identified for the project. According to EDUCAUSE IT Governance, Risk, and Compliance program the IT Risk Register is a sortable checklist that identifies common strategic IT risks and catalogues those risks according

to common risk types and IT domains. It also contains a resource to help institutions conduct a qualitative risk assessment of the items listed in the register.

No	Risk Statement	Risk Causes	Risk Impacts	Likelihood	Score
1	IT governance and priorities not aligned with institutional priorities	IT failure to understand institutional strategy; lack of institutional support for IT operations	Poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; inefficiencies and duplication of effort; poor perception/reputation of enterprise IT		
2	Failure to designate leadership (e.g., an individual or individuals) for institutional oversight and strategic direction for IT operations	Lack of institutional support for IT operations	Poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; creation of fiefdoms leading to inefficiencies and duplication of effort		
3	Failure to designate leadership (e.g., an individual or individuals) for institutional oversight and strategic direction	Lack of institutional support for IT and information security operations	Poor governance of enterprise information security efforts; inability to enhance, improve, or increase the effectiveness of institutional information security; data breaches; failure to meet		

	for information security activities		regulatory compliance requirements; regulatory fines and expenses		
4	No succession plan for key institutional IT leaders (e.g., CIO, CISO, CTO, CPO, etc.)	Lack of institutional support for IT operations; human nature not to plan for succession activities; lack of qualified internal staff for succession planning	Leadership void in the event of separation of a key IT leader from the institution		
5	Relevant stakeholders not included in important IT investment decisions (e.g., priorities, technologies, new applications)	Lack of senior management support; stakeholders fail to understand IT investment decisions (or provision of IT services in general); inability to identify stakeholders	Uses of organization IT systems that contravene good investment decision making; poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; inefficiencies and duplication of effort; increased cost for providing IT services; poor perception/reputation of enterprise IT		
6	IT assets (e.g., hardware, devices, data, and software) and systems not prioritized based on their classification, criticality, and institutional value	Lack of senior management support; complexity of business processes and automated systems; lack of funding and tools for prioritization efforts; failure to update prioritization when conditions change; stakeholder failure to agree on resource prioritization	Multiple redundant resources in place (inefficient and costly for the institution); lack of institutional knowledge about where IT resources, systems, and data are located; inability to implement business continuity plans to support institutional operations; financial losses due to replacement of nonpriority systems;		

			inability to execute strategic projects		
7	IT assets (e.g., hardware, devices, data, and software), systems, and services outdated, do not support institutional needs (admissions, academic, business operations, research, etc.)	Complex and inflexible institutional enterprise IT architecture (not scalable for current needs); failure to adopt new IT infrastructure and/or services in a timely manner to support institutional needs	Poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to provide needed business, academic, research services; inability to enhance, improve, or increase the provision of enterprise IT operations; increased cost for providing IT services; failure to support user IT needs; poor perception/reputation of enterprise IT		
8	IT management aims and directions not communicated to critical user areas	Lack of senior management support; failure to understand IT management priorities; failure to prioritize communications to critical user areas; lack of multiple communication channels (e.g., e-mail, print media, other electronic media) to convey information to user areas; failure of users to pay attention	Uses of organizational IT systems that contravene management aims; poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; inefficiencies and duplication of effort; poor perception/reputation of enterprise IT		
9	Lack of shared understanding by IT and business units that affects IT service delivery and projects	Lack of senior management support; failure of IT staff to understand business processes and how IT services can benefit	Inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the		

		those process; failure of business staff to understand IT processes; inability to identify and document business processes; mutual disrespect	community); inability to enhance, improve, or increase the provision of enterprise IT operations to support business, academic, or research processes; increased cost for providing IT services; failure of business process reengineering; distrust between organizational units		
10	IT projects not managed in terms of budget, scheduling, scope, priority, and delivery	Lack of senior management support; complexity of IT systems; complexity of cross-institutional IT projects; failure to assign a project manager or implement project management methodologies when engaging in IT projects; failure to inform stakeholders about project changes	Poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; increased cost for providing IT services; failure of IT projects; poor perception/reputation of enterprise IT		
11	No process for identifying and allocating costs attributable to IT services	Lack of senior management support; complexity of IT systems; complexity of institutional cost-allocation process; inability to calculate TCO of providing IT services; failure to account for indirect costs such as software license and upgrade fees	Poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; increased cost for providing IT services		
12	No process for measuring and managing IT performance	Lack of senior management support; complexity of IT infrastructure; lack of funding and tools for performance	Poor governance of enterprise IT; inability to use IT to strategically support institutional mission (admissions, research, institutional		

		management or metrics; insufficient staff to attend to performance management; failure to inform institutional audience about performance management	operations, outreach to the community); inability to enhance, improve, or increase the provision of enterprise IT operations; increased cost for providing IT services		
13	No process for managing IT problems to ensure they are adequately resolved or for investigating causes to prevent recurrence	Lack of senior management support; complexity of IT infrastructure; lack of funding and tools for service management; insufficient staff to attend to service management; failure to inform institutional audience about support processes; insufficiently skilled staff to investigate and resolve problems	Unable to address user problems in IT systems in a reliable manner; inefficient processing of support tasks (failure to gain efficiencies by tracking similar issues); inability to identify recurring issues; inability to prioritize support requisitions; failure to support business and academic processes; poor perception/reputation of IT		
14	Incorrect information on public-facing institutional resources (e.g., website, social media streams)	Information on public websites out of date; internal posting mistakes made by staff; intentional or unintentional vandalism	Institutional website unavailable for a period of time; staff and resource costs to repair website; institutional reputation loss; poor perception/reputation of IT		
15	Critical institutional business and academic data (e.g., admissions, business operations, research, etc.) not available when needed	Hardware failure; software failure; data deleted; facility destroyed; equipment lost/misplaced/stolen; lack of adequate backups; lack of source documents or input files; data on backups corrupted; backups unavailable (e.g., lost, stolen, missing); failure to make appropriate arrangements with	Failure of business processes (e.g., payroll, tax, HR functions); inability to execute on institutional mission; inability to participate in research activities; costs of outsourcing functions for a period of time; costs to recover data; regulatory implications for failure to meet legal or contractual requirements; institutional reputation		

		vendors to provide redundant or support services; lack of understanding recovery point objective (RPO—how much data can be lost and recreated); failure to conduct, maintain, and periodically test backups	loss; poor perception/reputation of IT		
16	Loss of access—for an unacceptable period of time—to IT systems and services hosted by another organization	Internet or campus network failure; hardware failure; software failure; data deleted; facility destroyed; equipment lost/misplaced/stolen (can be on the part of vendor or on institutional systems that interact with vendor systems); failure of authentication systems (vendor or institution); failure to make appropriate arrangements with vendors to provide redundant or support services; failure to develop and update business continuity strategies; failure to test business continuity plans; establishing unrealistic recovery time objectives (RTOs); lack of understanding of specific business objectives and critical processes	Failure of business, academic, or research processes; inability to execute on institutional mission; costs of outsourcing functions for a period of time; costs to recover data; regulatory implications for failure to meet legal or contractual requirements; institutional reputation loss; poor perception/reputation of IT		
17	IT communications and networks not	Internet or campus network failure; hardware failure;	Loss of communications within and beyond campus network; failure		

	protected from complete or intermittent failure	software failure; facilities destroyed; equipment lost/misplaced/stolen; intentional or unintentional vandalism; lack of redundant systems or IT resources; lack of funding to support redundancy; failure to develop and update business continuity strategies; failure to test business continuity plans	of IT services; failure of emergency notification services; institutional reputation loss; poor perception/reputation of IT		
18	Areas housing critical IT assets (e.g., hardware, devices, data, and software) or services physically inaccessible, inoperable, or unsuitable for human access	Smoke, biological or chemical agents, asbestos, other hazards; lock failures; intentional or unintentional vandalism; natural disaster damage; access to facility not controlled	IT personnel unable to access an area; emergency responders unable to access an area; unauthorized personnel possibly able to access the area; IT systems disabled or tampered with; failure of IT systems; theft of critical IT systems; theft of institutional data; unable to bring IT or other critical systems back online; destruction of backups of software, configurations, data, or logs		
19	Failure to make adequate plans for continuation of institutional business processes (e.g., admissions, academic, operational activities, and research) in the event of an extended IT outage	Hardware failure; software failure; data deleted; facility destroyed; equipment lost/misplaced/stolen; lack of senior management support; complexity of business processes and automated systems; lack of funding and tools to support continuity planning efforts;	Unable to recover systems and data to support business, academic, and research processes and activities in a timely manner; staff unable to understand roles/responsibilities; staff and resource expense to return to operations; failure to support institutional mission; institutional reputation loss; poor		

		failure to update business continuity strategies; failure to test business continuity plans; failure to ensure staff understand roles and responsibilities; failure to incorporate lessons learned into strategies; failure to address all phases of business continuity; establishing unrealistic recovery time objectives (RTOs); lack of understanding of specific business objectives and critical processes; lack of prioritization of critical business and IT processes; failure to make appropriate arrangements with vendors to provide redundant or support services	perception/reputation of IT		
20	No coordinated vetting and review process for third-party or cloud-computing services used to store, process, or transmit institutional data	Lack of senior management support; lack of communication of central vetting process to staff/employees; failure to understand the need to protect institutional data	Multiple redundant services in place (inefficient and costly for the institution); institution unaware who its business partners are; institution unaware if institutional data are held by third parties; institution unable to ensure that third parties are following compliance requirements		
21	Failure to create and maintain sufficient and current policies and standards to protect the	Lack of senior management support; failure to understand information security concepts; lack of funding to support	Improper use of organization IT systems and institutional data; failure of users to protect critical institutional data when using IT resources		

	confidentiality, integrity, and availability of institutional data and IT resources (e.g., hardware, devices, data, and software)	policy development activities; lack of funding for training; lack of user training	(leading to data breach); institution subject to regulatory violations and fines; institutional reputation loss; poor perception/reputation of IT		
22	Data breach or leak of sensitive information (e.g., academic, business, or research data)	Lack of senior management support; complex regulatory environments impacting organization IT systems and data (e.g., FERPA, HIPAA, GLBA, PCI, accessibility, export controls, etc.); complexity of IT systems, infrastructure, and services; lack of funding for data handling training; lack of user training; intentional user malfeasance; unintentional user error; hacking or infiltration by third parties	Institution subject to regulatory violations and fines; costs of breach notification; costs of redress for individuals; loss of alumni donations; loss of research data; costs to mitigate underlying breach event; institutional reputation loss; poor perception/reputation of IT		
23	Inadequate cyber security incident or event response	Lack of senior management support; complexity of business processes and automated systems; lack of funding and tools to support security incident response; failure to update incident response strategies; failure to test incident response plans; lack of staff with incident response expertise	Unable to recover systems and data to support business, academic, and research processes and activities in a timely manner; staff and resource expense to return to operations following a security incident; unable to assist in legal investigations related to an incident; institutional reputation loss; poor perception/reputation of IT		

24	Failure to control logical access and incorporate principles of least functionality to IT resources (e.g., hardware, devices, data, and software) and systems	Failure to use authentication systems; failure of authentication systems; authentication systems easily disabled; giving user access to more systems and assets than is needed to complete staff tasks; failure to remove access when user separates from the institution or changes job duties; lack of staff with identity management expertise	Unauthorized access to IT systems; IT systems disabled or tampered with; failure of IT systems; theft of critical IT systems; theft of institutional data; users mistakenly given more system access than is needed to complete job duties; inability to maintain the confidentiality of data in institutional systems		
25	Failure to control physical access to data centers/facilities and areas housing critical IT resources (e.g., hardware, devices, data, and software) and systems	Failure to use physical locks; failure of physical locks; physical locks easily disabled; failure to use authentication systems; failure of authentication systems; authentication systems easily disabled	Unauthorized access to facilities or IT systems; IT systems disabled or tampered with; failure of IT systems; theft of critical IT systems; theft of institutional data		
26	Failure to follow organized life-cycle management practices (development, acquisition, use, transfer, repair, replacement, destruction) for institutional IT resources and systems	Lack of senior management support; complexity of IT processes and systems; lack of funding and tools to support life-cycle management efforts; failure to update documentation when conditions change; insufficient staff to attend to task efforts; failure to train IT staff on life-cycle management	Multiple redundant resources in place (inefficient and costly for the institution); institution unaware where its IT resources and systems are located; institution unaware how its data are transmitted or where its data are; institution unaware if IT resources or institutional data are held by third parties; institution unable to ensure its own or third-party adherence		

		processes (including equipment removal and destruction, data deletion)	to compliance requirements; inability to support, prioritize, or understand criticality of systems for business continuity purposes; financial losses due to replacement of misplaced systems; regulatory fines for improper disposal of resources and/or data (data breach or toxic waste disposal); institutional reputation loss		
27	Failure to document institutional IT infrastructure architecture and to implement change-control processes (including creating, maintaining, and revising baseline IT system configurations)	Lack of senior management support; complexity of IT processes and systems; lack of funding and tools to support change-control processes and efforts; failure to update documentation when conditions change; insufficient staff to attend to task efforts; failure to train IT staff on change-control processes	Multiple redundant resources in place (inefficient and costly for the institution); inability to support, prioritize, or understand criticality of systems for business continuity purposes; inability to provide a baseline configuration of successful IT operations; failure to understand the effect of IT configuration changes on business system processes; multiple departments making uncoordinated changes to IT systems; financial losses due to duplicative changes and required rollbacks		
28	Institutional IT communication and data flows not documented	Lack of senior management support; complexity of IT processes and systems; lack of funding and tools for mapping efforts; failure to update maps/data flows when conditions change; insufficient	Multiple redundant services/communication flows in place (inefficient and costly for the institution); institution unaware how its data are transmitted or where its data are; institution unaware if institutional data are held by third parties; institution		

		staff to attend to task efforts	unable to ensure its own or third-party adherence to compliance requirements; inability to support, prioritize, or understand criticality of systems for business continuity purposes		
29	Licenses and permits for institutional IT systems and software not maintained	Lack of senior management support; complexity of IT infrastructure and software licensing requirements; lack of funding and tools for licensing management; insufficient staff to attend to acquisition efforts; failure to train IT staff on the need for software/hardware licenses	Operation of IT resources and software in a manner that violates contractual terms; institution subject to contract liability; institutional reputation loss; poor perception/reputation of IT		
30	No process for ensuring institutional data remain complete, accurate, and valid during input, update, and storage	Lack of senior management support; complexity of business processes and automated systems; failure to ensure staff understand roles and responsibilities; failure to train staff on proper data entry; failure to incorporate automated processes to ensure valid data entry; failure to log data changes	Failure of business, academic, or research processes; inability to execute on institutional mission; costs of outsourcing functions for a period of time; costs to recover data; regulatory implications for failure to meet legal or contractual requirements; loss of integrity in automated systems		
31	Audit logs on critical IT systems and processes not maintained	Lack of senior management support; complexity of IT infrastructure; lack of funding and tools for log management; lack of space to store logs; lack of tools to review	Unable to understand and recreate anomalies experienced in IT systems; unable to perform forensic analysis		

		and manage log entries; insufficient staff to attend to log management;			
32	Too few IT staff to ensure continuous IT system operations	Inability to recruit and retain sufficient numbers of competent IT staff needed to support enterprise IT operations; failure to maintain the staffing levels or skill sets needed to support enterprise IT operations; any personal situation that renders personnel unable to attend to institutional duties (military service, family obligations, natural disaster, death); single expert in field separates from employment with institution; vendor personnel unavailable under similar scenarios as presented above; inability to be physically present on campus due to a natural disaster or civil disturbance	Inability to enhance, improve, or increase the provision of enterprise IT operations; unable to operate/recover systems and data to support to support business, academic, and research processes and activities; overreliance on key staff; low employee morale; increased employee turnover; failure to support institutional mission		
33	Users (e.g. staff, administrators, third parties) do not follow legal and regulatory requirements regarding the operation/use of IT systems and the use of institutional data	Lack of senior management support; complex regulatory environments impacting higher education IT systems and data (e.g., FERPA, HIPAA, GLBA, PCI, accessibility, export controls, etc.); lack of	Improper use of university IT systems and organizational data; failure of users to protect critical institutional data when using IT resources (leading to data breach); organizational subject to regulatory violations and fines; institutional reputation loss		

		funding for training; lack of user training			
34	Users (e.g. staff, administrators, third parties) do not follow organizational policies regarding the operation/use of IT systems and the use of institutional data	Lack of senior management support; complex organization policies impacting organizational IT systems and data; lack of funding for training; lack of user training	Improper use of organization IT systems and institutional data; failure of users to protect critical institutional data when using IT resources (leading to data breach); institution subject to regulatory violations and fines; institutional reputation loss		