



# Connecting CTOs & CBOs: Building Bridges for Institutional Success

Welcome to today's discussion on strategic collaboration between Chief Technology Officers and Chief Business Officers. We'll explore critical integration points that strengthen our institutions.



# CBO-CTO Partnership



## **Executive Representation**

Ensure technology has a "seat at the table" in leadership discussions.



## **Effective Communication**

Maintain open dialogue about priorities and challenges.



## **Strategic Partnership**

View IT as partners rather than a "job shop" for technology tasks.



## **Shared Risk Management**

Collaborate on cybersecurity and technology risk mitigation.

# Technology's Dual Role

## Educational Technology

Unlocks learning boundaries and simplifies resource access.

Promotes personalized learning experiences.

Removes physical barriers through on-demand options.

## Enterprise Technology

Improves productivity and operational efficiency.

Automates critical organizational processes.

Manages infrastructure and enables growth.



# Educational Technology Ecosystem

## **Learning Management Systems**

Centralized platforms for course delivery, content management, and student engagement tracking.

## **Student Support Systems**

Library resources, tutoring platforms, and early alert tools that enhance student success.

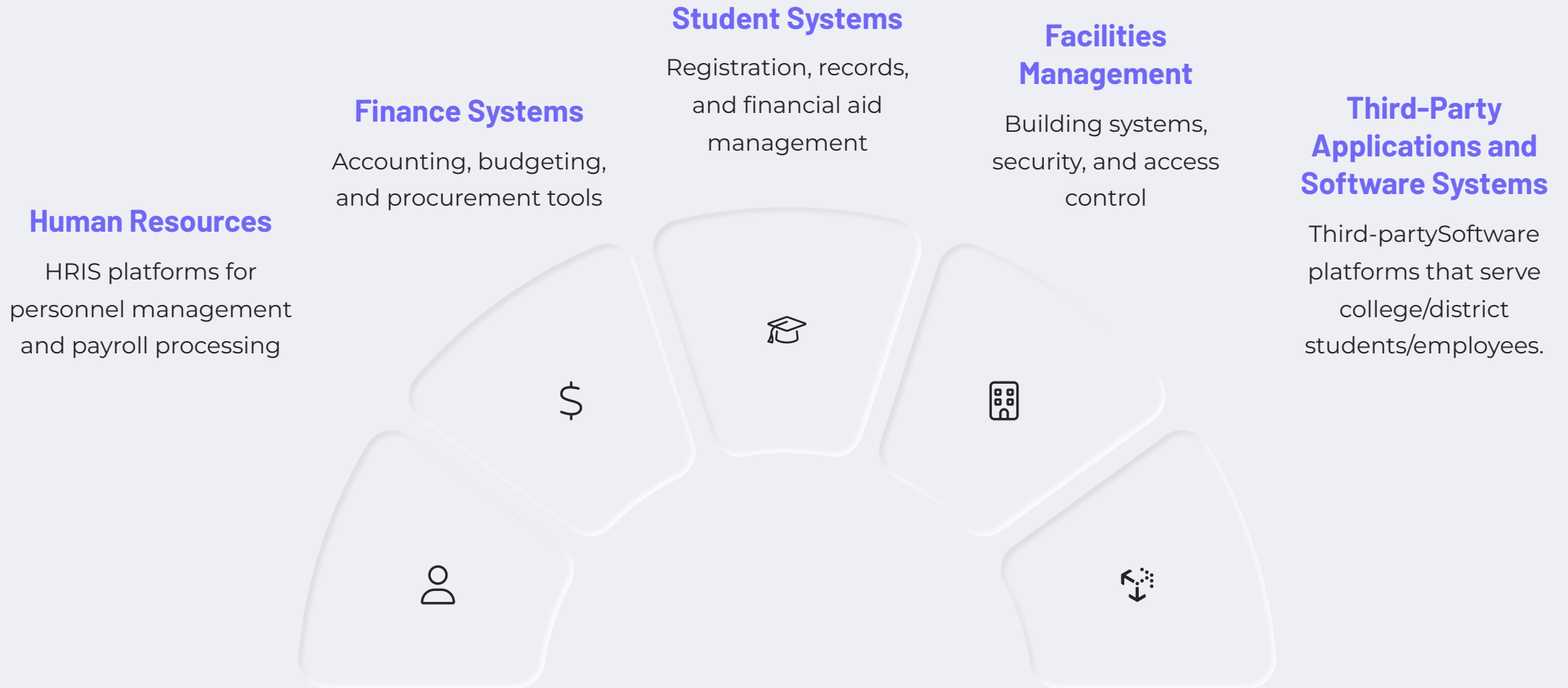
## **Administrative Tools**

Counseling and scheduling systems that streamline student services and improve accessibility.

## **Physical Learning Spaces**

Smart/multimedia classrooms, common areas on campus, study rooms, outdoor learning spaces.

# Enterprise Technology Portfolio



# Procurement Best Practices



## Early IT Involvement

Include technology leaders in purchasing discussions from the start



## Technology Sign-Off

Require IT review for all technology-related purchases



## Integration Planning

Evaluate how new systems connect with existing infrastructure

4

## Security Assessment

Review vendor security practices and data protection measures

**Collaboration: Purchasing/Procurement**

# Elevating the Purchasing Process through Collaboration

## Technology Review Benefits

- Ensures compliance with standards
- Validates security requirements
- Confirms accessibility compliance
- Verifies system compatibility
- Aligns with institutional tech portfolio

## Strategic Purchasing Solutions

- Reduces shadow IT proliferation
- Leverages CollegeBuys opportunities
- Optimizes RFP processes
- Coordinates enterprise contracts
- Collaboration on Board items for approval



# Financial System Collaboration



## System Maintenance

Coordinating patches and updates for Banner/Colleague/Workday systems.



## Process Automation

Creating workflows to streamline financial operations.



## Payment Integration

Implementing secure payment processing systems.



## Custom Reporting

Developing specialized fiscal reports with IT analysts.



# **Collaboration: Bond Programs**

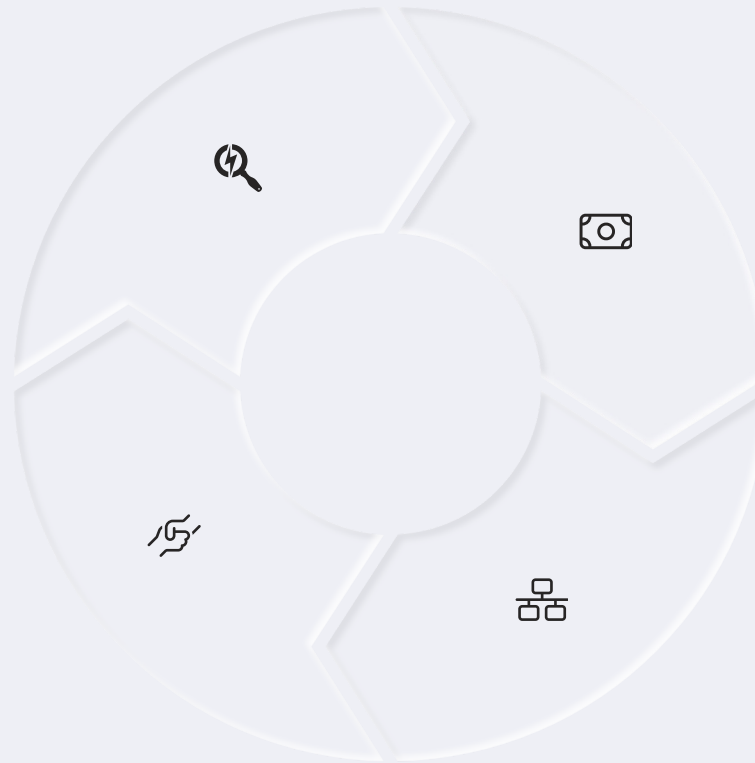
# Bond Program Partnership

## Needs Assessment

Identifying current and future technology requirements.

## Service Support

Providing technical expertise across initiatives.



## Budget Planning

Collaborating on financial forecasting and allocation.

## Infrastructure Projects

Implementing campus-wide technology improvements.

**Collaboration: Cybersecurity & Risk Management**

# Cybersecurity & Risk Management



Our collaborative approach to cybersecurity integrates IT expertise with business office risk management protocols, creating a unified defense strategy against ransomware, data breaches, and social engineering attacks while ensuring compliance with FERPA, GLBA, and other regulatory requirements.



# CYBERCRIME TRENDS THREATENING CALIFORNIA COMMUNITY COLLEGES

Unprecedented rise in cyber attacks targeting higher education

**880,418** FBI complaints in 2023 — up **9.6%**

Total losses reached **\$12.5 billion**





# CALIFORNIA'S HEIGHTENED VULNERABILITY

**80,000+**

**CA Complaints**

Highest of any state

**\$2B+**

**CA Losses**

Financial impact

**18%**

**Ransomware Increase**

Education heavily targeted

Source: FBI San Francisco Field Office Report, HIPAA Journal



# Business Email Compromise: What Is It?

BEC is a sophisticated scam targeting businesses with fraudulent email requests that appear legitimate.

## How It Works

Cybercriminals impersonate trusted contacts or executives to request urgent financial transactions.

## Real-World Example

A community college AP clerk receives an email from the "chancellor" requesting to update a vendor's routing number.

## The Damage

The clerk updates the account. When the real payment goes out, funds are routed to criminal accounts instead.



# BUSINESS EMAIL COMPROMISE: YOUR BIGGEST THREAT



**21,489 BEC incidents**

Most costly cybercrime category



**\$2.9B in losses**

From BEC attacks alone



**\$183,000 avg cost**

Double from 2022



**\$55B+ global impact**

Over the past decade

Sources: SC Media Analysis, CyberInsurer (NetDiligence Study), FBI PSA (Sept 2024)



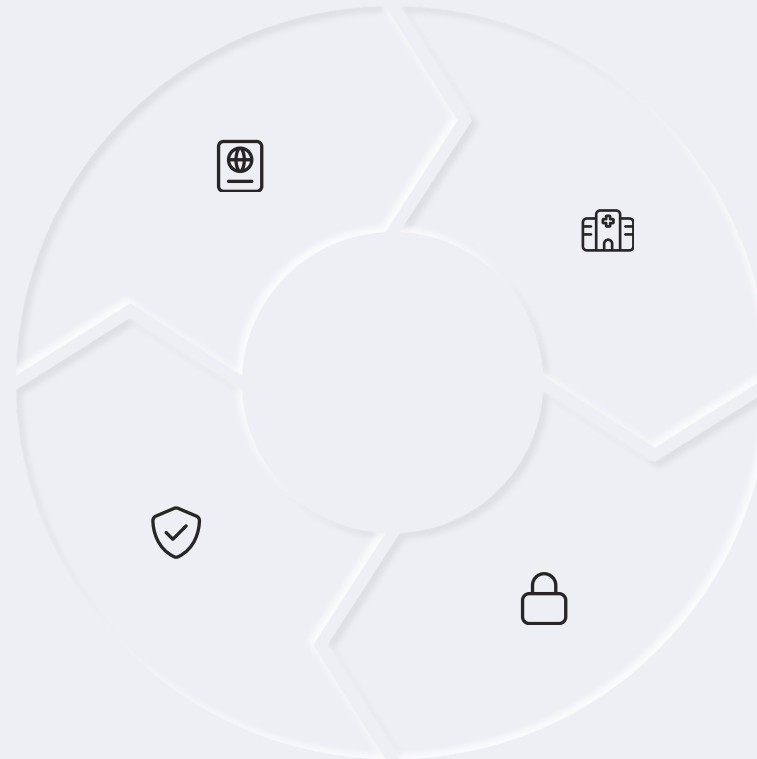
# FINANCIAL CRIME RED FLAGS

## 4.6M SARs Filed Annually

Financial institutions filed 12,600 suspicious activity reports daily, with 22% involving educational institutions in California

## Resource Gap Exposure

73% of CA community colleges reported insufficient cybersecurity staffing and 68% lack adequate threat detection tools



## California Colleges Under Attack

Education sector saw 47% increase in targeted attacks, ranking second only to healthcare (53%) in 2023

## \$59.6M CA Ransomware Losses

Community colleges accounted for \$12.3M in losses when systems were held hostage, disrupting operations for 14-21 days on average

Sources: American Bankers Association, Axios Report, California Community College Information Security Center

**Collaboration: Regulatory Compliance & Audit**

# Regulatory Compliance

## 1 FERPA Implementation

Collaborating to develop comprehensive data classification systems, role-based access controls, and audit trails for student records. Includes annual staff certification and documented release procedures.

## 3 GLBA Safeguards

Establishing risk assessment frameworks, incident response protocols, and vendor management processes for financial data protection. Includes regular security posture evaluations and documentation reviews.

## 5 Annual Audit for IT

An IT audit is included as part of the annual external audit process. Auditors work with IT to review documentation and practices such as internal controls, IT change controls, security and access controls, district policies, and various audit tests.

## California, Federal, and International Regulations

California privacy and data security laws, California Public Records Act requests, Federal rules governing information security, breach notification laws, Federal Financial Aid guidelines, and international regulations such as GDPR compliance

1

2

## PCI Standards and Penetration Testing

Implementing tokenization, end-to-end encryption, and network segmentation for campus payment systems. Requires coordinated regular vulnerability scanning and penetration testing for college systems and networks.

3

4

## HIPAA Security

Developing encrypted communication channels, secure health record repositories, and disaster recovery plans for campus health services. Includes privacy impact assessments and breach notification procedures.

5

6

## Information Security Program

Now required by GLBA, includes a comprehensive information security program with mandatory components such as privacy and safeguard measures, incident response process documentation, procedures for regular system scans and tests, and includes an annual board presentation on cybersecurity.

7

# **Collaboration: Enrollment & Funding Strategy**



# Enrollment Strategy & Financial Forecasting

## System Support Assessment

Evaluating if current technologies advance or impede enrollment and revenue initiatives.

## Advanced Analytics

Implementing AI-powered tools that enhance scenario planning beyond ERP capabilities.

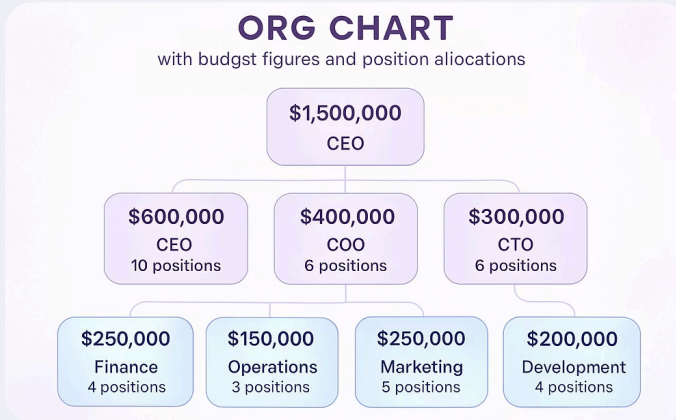
## Data Integration

Creating unified views across systems for comprehensive financial modeling.



# **Collaboration: Fiscal & HR Crossover**

# Connecting Fiscal & HR Operations



## Position Control

Managing budgeting for funded positions



## Salary Planning

Implementing COLA and compensation adjustments



## Process Automation

Streamlining workflows between departments

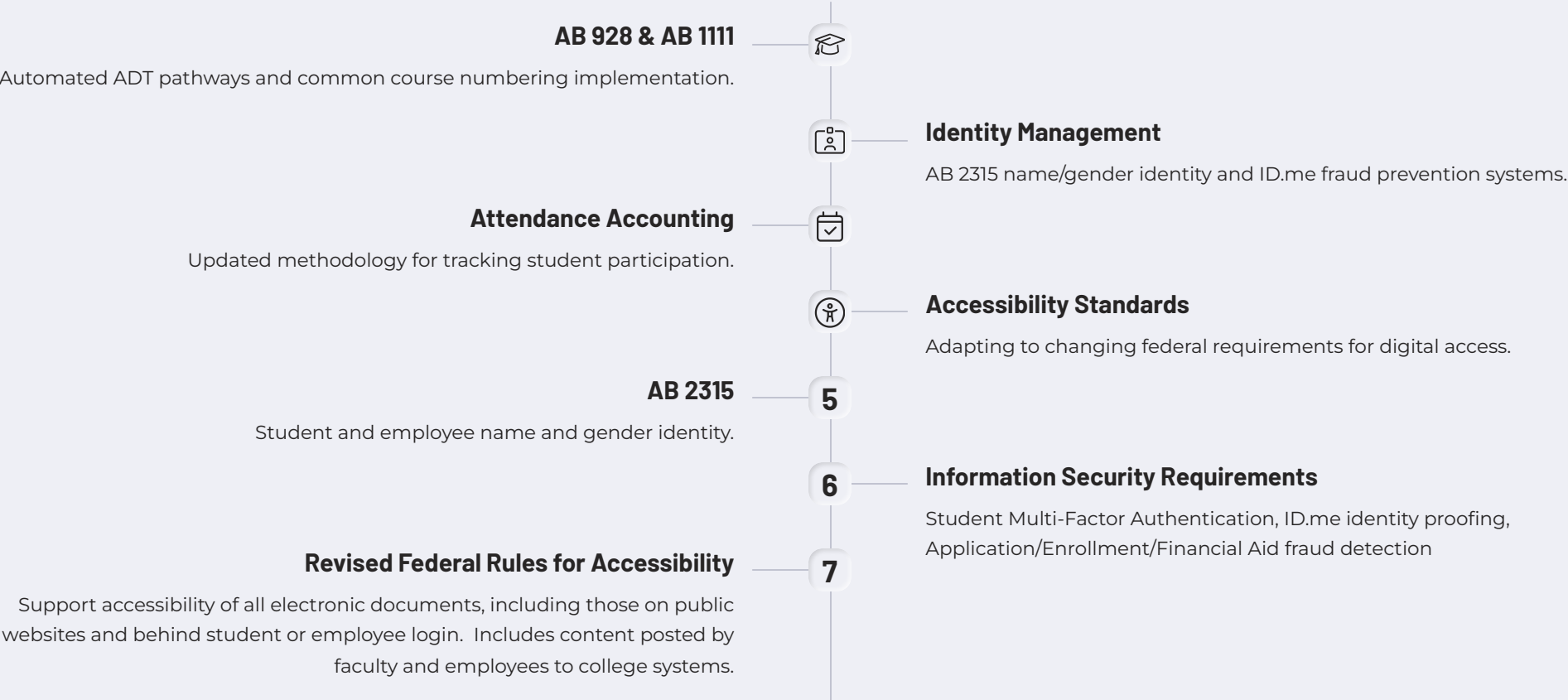
IT serves as the crucial bridge between fiscal and human resources functions, providing both consulting expertise and system integration solutions.



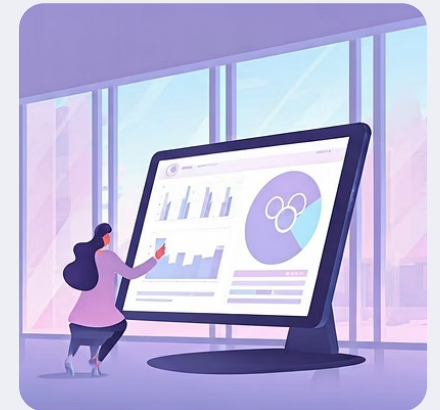
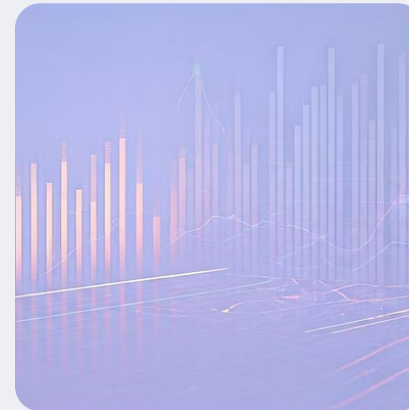
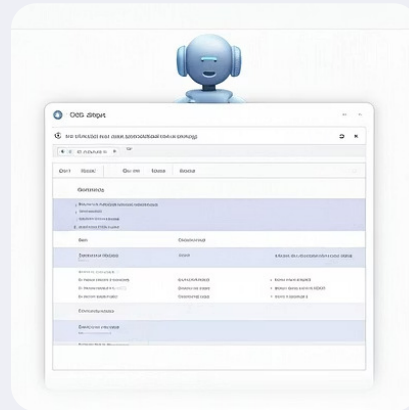
## **Collaboration: New Initiatives & Mandates**



# Implementing New Mandates



# The AI Revolution



AI tools are rapidly evolving, offering new capabilities for data analysis, automation, and decision support in higher education administration.



# Statewide Innovation Initiatives



## **Common Cloud Data Platform**

Streamlining MIS reporting and enabling future AI innovations



## **HUMANS AI Framework**

Ethical guidelines for AI implementation in education



## **Digital Innovation Center**

Coordinating transformation and equity initiatives



## **Future Pilots**

Opportunities for finance and institutional support innovations



# AI Applications in Finance

## Data Analytics

Drive deeper insights through pattern recognition and automated analysis.

## Predictive Forecasting

Generate more accurate enrollment and revenue projections.

## Process Automation

Streamline routine transactions and approval workflows.

## Enhanced Reporting

Create dynamic visualizations and real-time data access.



# AI Implementation Considerations

## Data Privacy

Protecting sensitive institutional and student data is paramount for compliance and trust.

## Staff Training

Developing internal capability ensures sustainable adoption and proper usage.

## Integration Complexity

Connecting AI tools with existing systems requires careful planning and architecture.

## Cost Factors

Implementation and ongoing costs must be balanced against expected returns.

## Ethical Guidelines

Ensuring AI use aligns with institutional values and avoids bias or harm.

Successful AI implementation requires balancing technical capability with ethical considerations and staff readiness.



# Your Call to Action



## Build Tech Partnerships

Strengthen your working relationship with technology leaders at your institution.



## Develop AI Literacy

Commit to ongoing learning about AI applications in higher education finance.



## Champion Innovation

Identify one process in your area that could benefit from AI enhancement.

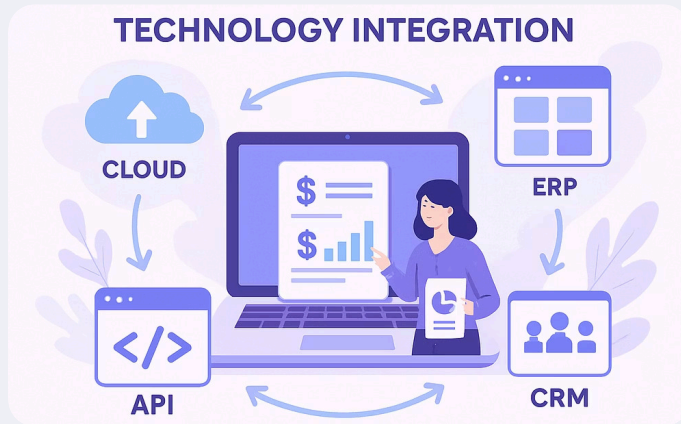


## Prioritize Security

Review your current risk management approach with your technology team.

# Moving Forward Together

Building successful partnerships through technology and collaboration



## System Integration

Full technology alignment with fiscal goals



## Cost Reduction

Generate savings through strategic collaboration



## Operational Efficiency

Improvement through coordinated planning



# Contact Information

Jory Hadsell

Vice Chancellor & CTO at Foothill-De Anza CCD  
hadselljory@fhda.edu

Executive in Residence - Strategic Technology Initiatives  
jhadsell@cccco.edu