Technical Requirements

1. Please provide an overview of the system products your company offers.
    a. Indicate if any of the products offered in your solution are provided to you from a third party (i.e., are non-native to your core product code). Provide the third-party's name. Briefly describe the level of integration between your core technology and third-party add-ons.
2. Are we required to purchase any additional software other than what is acquired from you? Please list those required and those recommended.
3. Describe the network requirements and set up to allow us to access the application, including ports, protocols, CDN, and IPs.
4. Please state your solution's interface compatibility and past integration history with Ellucian Banner.
5. Please state your solution's integration capabilities with third party web conferencing solutions.
6. What technologies are planned for future use?
7. Does your system offer a Web Services API to facilitate integration with other systems?
8. Describe the process to connect to the back-end database.
9. Please describe the system's reporting capabilities, including the following:
    a. Remote reporting capabilities using tools such as Power BI, eVisions Argos, etc.
    b. Self-service report writing capabilities with data export to .csv or .xlxs
    c. Automated daily report capabilities
10. In what format is data imported and/or exported?
11. Describe your software lifecycle development methodology.
12. Describe your QA process and approach to continuous improvement.
13. How do you monitor the Quality of Work provided by your team? Include specific measurements.
14. Please describe your procedures for taking corrective action when customers express dissatisfaction with deliverables.

System/Software Support

1. Please describe your Customer Support policy. Include information about response times, escalation policies, and hours of operation.
    a. What is the response time for critical (system down, etc…) issues?
    b. What is the response time for standard (non-down) issues?
2. Can users and administrators contact Support representatives via e-mail or log inquiries online during non-business hours?
3. Is support available for extended (e.g., 24x7) hours?
    a. If yes, is there an additional cost for this service?
4. What is your escalation process?
5. How frequently do upgrades occur? Describe a typical upgrade process.
6. What is your release support policy?
7. Is your Help Desk outsourced? If yes, with which countries?
8. How is knowledge transferred from your team to the College's ongoing support team?

9. Please upload and include a detailed Service Level Agreement (SLA) document with your RFP. The SLA should include downtime allowances (standard windows for maintenance), high volume usage response times and disaster recovery. If you offer multiple SLA options, please include details and prices for those options. The SLA details should include the associated penalties or credit given for exceeding the SLA terms.
10. Describe the methods that are used to backup client data. Make sure to address the following questions in your response:
    a. How is client data backed up?
    b. How frequently is client data backed up?
    c. Where are the backup files stored?
    d. Do clients have the right to request backup data, in a usable format, a set number of times per year?

Security and Risk Requirements

If you provided a detailed response to any of the questions below in your HECVAT, please feel free to reference us back to the section in the HECVAT document that was submitted.

1. Describe your security model, including network, data, and application security, data center security, application and system support, upgrades and maintenance, and personnel access rights.
2. Describe your methodology and practice regarding patching and/or updating your application software.
3. How do you handle critical vulnerabilities, such as Log4j?
4. Describe your procedures for application/system incident response including the submission of found vulnerabilities.
5. Describe your procedure for incident monitoring and response. When is the customer notified?
6. How do you monitor system integrity, logs, intrusion detection, and system access (e.g., checking the logs to verify failed and successful logins, password changes)?
7. Describe the system's security methodology to ensure that only authorized users can access information about disciplinary action.
8. Does the system have auditing capabilities (e.g., capture information whenever a content object is accessed to help the organization reduce compliance risk)?
9. Can the organization control which functions are enabled?
10. Do you have scheduled penetration tests to verify your security? If yes, then please summarize the results of your last test, as well as any follow-up actions that were taken to mitigate risk.
11. Describe your disaster recovery process, including:
    a. Your disaster recovery procedures
    b. When do you perform disaster recovery tests?
        i. If yes, how often?
12. Describe how client data is protected, both physically and at the system level.
13. Are there scheduled security audits of your infrastructure?
14. Is your data center ISO/IEC 27001:2013 compliant?
15. Have you had a SAS70/SSAE16/SSAE18 audit of your data center in the last year?

    a. Please provide us with your latest SAS 70/SSAE16/SSAE18 audit results.
    b. Please provide us with proof of compliance to the FTC Red Flag Rules.
16. Please describe the Identity Management options (e.g., SSO, etc.) that you support.
17. Does your system support local and/or admin accounts? If yes, then how are those accounts secured within the platform?
18. Please describe how your system handles and supports multi-factor authentication (MFA).
19. Describe your approach to risk management.
20. Who owns the data in your system?
    a. If we do not renew an agreement, how do we obtain our data in a usable format?
        i. How quickly will this data transfer occur?
    b. After we receive and verify the final copy of our data, how do you ensure that our data has been removed from your servers?

Regulatory Compliance

The System must protect the customer's educational and financial information and must meet the requirements of all applicable federal regulations, including but not limited to: the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Americans with Disability Act (ADA), FTC Red Flag Rule and Payment Card Industry Data Security Standards (PCI).

1. Please explain any regulatory or compliance impact to the college as it pertains to the use of your system.
2. Please explain how all compliance requirement status will be communicated annually to the college.
3. Please explain how audit reports will be communicated annually to the college.